

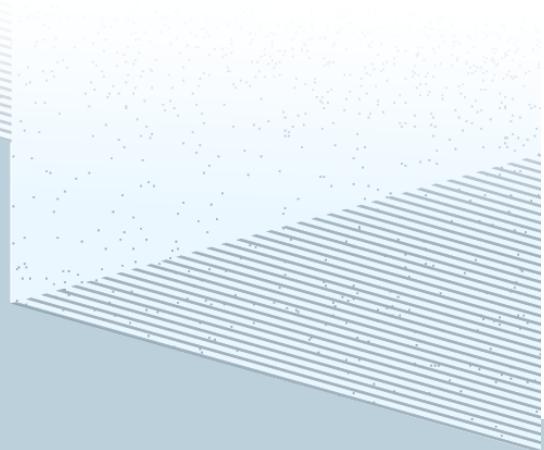
THESE DE DOCTORAT DE

L'UNIVERSITE DE RENNES 1
COMUE UNIVERSITE BRETAGNE LOIRE

ECOLE DOCTORALE N° 599
Droit et Science politique
Spécialité : *Science politique*

Par

Yves Auffret



Relations Internationales et cyberespace, théories et acteurs asymétriques
Etude pragmatique de la sécurité de l'information par l'analyse de discours

TOME 1 – Introduction, chapitre liminaire, première partie.

Thèse présentée et soutenue à Rennes, le 6 novembre 2019

Unité de recherche : Institut du Droit Public et de la Science Politique, UR1_RS438

Rapporteurs avant soutenance :

THIERRY BALZACQ
Professeur à l'Institut d'Etudes Politiques de Paris

JEAN-VINCENT HOLEINDRE
Professeur à l'Université Paris II, Panthéon-Assas

Composition du Jury :

THIERRY BALZACQ
Professeur à l'Institut d'Etudes Politiques de Paris

JEAN-VINCENT HOLEINDRE
Professeur à l'université Paris II, Panthéon-Assas

FREDERIC LAMBERT
Professeur à l'université de Rennes 1

JENNY RAFLIK-GRENOUILLEAU
Professeure à l'Université de Nantes

Directeur de thèse
BERNARD BRUNETEAU
Professeur à l'université de Rennes 1

Université de Rennes 1
ECOLE DOCTORALE N° 599 – Droit et Science politique

**RELATIONS INTERNATIONALES ET CYBERESPACE
THEORIES ET ACTEURS ASYMETRIQUES**

Etude pragmatique de la sécurité de l'information par l'analyse de discours

TOME 1 – Introduction, chapitre liminaire, première partie.

Par Yves Auffret

Thèse présentée en vue de l'obtention du doctorat en Science Politique

Sous la direction du Professeur Bernard Bruneteau

Membres du jury :

M. Thierry Balzacq, Professeur à l’Institut d’Etudes Politiques de Paris (rapporteur)

M. Jean-Vincent Holeindre, Professeur à l’université Paris II, Panthéon-Assas (rapporteur)

M. Frédéric Lambert, Professeur à l’université de Rennes 1

Mme Jenny Raflik-Grenouilleau, Professeure à l’université de Nantes

M. Bernard Bruneteau, Professeur à l’université de Rennes 1 (directeur)

6 novembre 2019

Convention d'écriture

L'ensemble composé du terme de « cyberspace » ainsi que des variations de celui-ci, et leurs pluriels, seront écrit d'un seul tenant. Le tiret ne sera pas utilisé dans ce cadre, sauf deux exceptions :

Lorsqu'un auteur d'une œuvre a lui-même utilisé le tiret dans le titre de sa production.

Et pour désigner le préfixe « cyber- » et le distinguer de l'adjectif « cyber » qui peut être utilisé dans certaines expressions.

Réserve de responsabilité

L'université de Rennes 1 et le ministère des Armées n'entendent donner ni approbation ni improbation aux idées émises dans les mémoires et autres documents soutenus en vue de l'obtention de grades universitaires et diplômes. Ces opinions doivent être considérées comme propres à leurs auteurs et n'expriment en rien la position des institutions auxquelles ils appartiennent.

Remerciements

Je remercie chaleureusement toutes les personnes qui m'ont aidé pendant l'élaboration de ma thèse et en particulier mon directeur, Bernard Bruneteau, pour sa bienveillance, son intérêt depuis mon tout premier mémoire en Master I, son soutien durant ces années, ainsi que l'autonomie à laquelle il m'aura permis d'accéder.

Ce travail n'aurait pas été possible sans le soutien de l'Armée de l'Air et du Centre de Recherche de l'Ecole de l'Air qui m'ont permis, grâce à un engagement en tant qu'officier sous contrat, de me consacrer presque sereinement à l'élaboration de ma thèse. Je tiens à remercier l'IDPSP de Rennes et le CREA de Salon-de-Provence pour l'accueil et les conditions de travail privilégiées qui m'ont été offertes, et tout particulièrement les quatre directeurs que j'y ai côtoyés, les colonels Viaud et Raout, ainsi que les Professeurs Le Floch et Gicquel. Je remercie Brigitte Deneuville et Isabelle Clerc pour leurs indéfectibles soutiens.

Cette thèse est également le fruit des nombreuses rencontres intellectuelles qui m'ont fait progresser tout du long de son élaboration. Je tiens à remercier Christophe Pajon pour son aide, ses conseils, ses encouragements et sa relecture toujours attentive. Je remercie également tous les enseignants qui m'ont aidé à accéder à mon terrain, en particulier Frédéric Douzet et Daniel Ventre. Merci également, à tous ceux avec qui j'ai eu la chance d'échanger durant cette thèse, à Rennes ou ailleurs.

Je remercie également mes collègues de la Base Aérienne 701 qui m'ont aidé à faire face durant ces années : Pierre Barbaroux, Colin Blattler, Cyril Camachon, Daniel Gigan, Ludovic Fabre, Anne-Lise Marchand... Je remercie mes collègues (ex)doctorants de Salon, de Rennes et des alentours notamment : Emilien Dubois, Camille Trotoux, David Helleu, Thomas Marcouf, Guillaume Muller, Bertrand Kirch, Azza Chaouch Bouraoui, Jean Roger, Jean-Philippe Hias, Frédéric Roggero, Quentin Wald, Gregory Froger, Albéric Perrier, Julien Augustyn, Alan Tymen... Je remercie particulièrement mes indéfectibles complices en organisation de colloques Alexis Robin et Matthieu Le Verge. J'adresse enfin mes remerciements à mes proches qui m'ont soutenu et supporté dans tous les sens du terme durant ces années. Merci à eux d'avoir compris mes trop nombreuses absences. Merci à Frédéric, Manu, Aby, Mathieu, Corentin, Alex, Ludovic, Marion, Mathilde... Merci à eux, et merci aux nombreuses autres personnes que cette seule page m'empêche de nommer.

Merci à ma famille. Merci tout particulièrement à ma mère et à ma sœur, Morgane. Et enfin, et surtout, merci à Orane pour m'avoir soutenu quotidiennement du début à la fin.

Je dédie cette thèse à ma grand-mère, Marie-Thérèse Cariou (1923 – 2012).

Sommaire

Tome 1

Sommaire	7
Liste des illustrations	10
Introduction générale	12
Chapitre liminaire – Stratégie, méthode et conduite de la recherche.....	24
Section 1 – Théories des Relations Internationales : des paradigmes à la combinaison pragmatique.....	26
Section 2 – Les mots et les discours : De l’efficacité politique du langage à l’objectivation rhétorique du politique.....	50
Section 3 – Dépasser le nominalisme : Etude de discours et approche phénoménologique plurielle du « cyberespace ».....	83
Section 4 – Entre phénomène discursif et combinaison pragmatique, l’apport d’une méthode de travail abductive.....	104
Section 5 – Du doctorant à l’officier : regard critique sur un parcours doctoral engagé... 108	
Section 6 – Evolution des contraintes matérielles et scientifiques de la recherche.	113
Partie I – Du mot au discours, le tournant sécuritaire du cyberespace : Eviter les pièges de la recherche d’une définition unique.....	122
Chapitre 1 – Circulations et mutations du cyberespace : un objet hors de la technique ?	124
Section 1 – Aux sources du pouvoir évocateur du cyberespace, invention, héritages et confusions.	128
Section 2 – Le cyberespace comme discours ambigu sur les technologies de l’information.	146
Section 3 – Une nécessaire méfiance envers les tentatives de définitions du cyberespace et des termes dérivés.	183
Conclusions de chapitre.	194
Chapitre 2 – Cyberespace et termes dérivés : analyse logométrique multiniveaux entre 2001 et 2016.	197

Section 1 – Discours « cyber » et impact normatif des enjeux sécuritaires de l’information (France, UE, ONU)	199
Section 2 – La thématique « cyber » dans la presse écrite francophone :	231
Section 3 – Eléments de discussion du phénomène discursif « cyber ».....	247
Conclusions de chapitre.	266
Chapitre 3 – Le phénomène linguistique « cyber » : la communauté épistémique comme communauté discursive.....	268
Section 1 – De l’émergence de la production d’une communauté épistémique dans le champ sémantique.	269
Section 2 – Les frontières normatives de la sécurité de l’information.	285
Section 3 – La place du phénomène linguistique « cyber » dans les enjeux de sécurité de l’information en France.....	305
Conclusions de chapitre.	333
Conclusions partielles.	335

Tome 2

Partie II – Sécurité de l’information dans les Relations Internationales : De l’enjeu de sécurité à un acteur en réseau.....	343
Chapitre 4 – Le cyberespace, un discours de sécurité consacré à l’information parmi d’autres.	345
Section 1 – Des éléments du discours : menace, dépendance, valorisation de l’information.	346
Section 2 – Théories pour une approche discursive du cyberespace et de la sécurité de l’information.	364
Section 3 – La réception des discours sur la sécurité de l’information dans les Relations Internationales.....	388
Conclusions de chapitre.	432
Chapitre 5 – Au-delà du discours, étudier les Relations Internationales par la sécurité de l’information.....	435
Section 1 – Les questions de la sécurité de l’information aux Relations Internationales..	436
Section 2 – Comprendre l’information dans l’étude des Relations Internationales.....	463

Conclusions de chapitre	478
Conclusion générale.....	481
Table des matières.....	490
Bibliographie	513
Index des noms d'auteurs.....	560

Liste des illustrations

Chapitre liminaire – Stratégie, méthode et conduite de la recherche.....	24
Figure 1 – Résumé des outils du pragmatisme conduit par les problèmes et des causes de non-pertinence des explications.	49
Figure 2 – Résumé de la conceptualisation de l’objet par une approche discursive.....	82
Figure 3 – Processus de recherche global avec ajout de la démarche abductive.....	106
Chapitre 1 – Circulations et mutations du cyberespace : un objet hors de la technique ?.....	124
Figure 4 – Rappel sur l’origine des premiers termes voisins ou dérivés de la cybernétique.	129
Chapitre 2 – Cyberespace et termes dérivés : analyse logométrique multiniveaux entre 2001 et 2016.	197
Figure 5 – Descriptif du corpus d’étude « Cyber JO RF 2001–2016 ».	200
Figure 6 – Recensement des occurrences des termes « cyber ». Corpus n°1	202
Figure 8 – Chi2 – Classification hiérarchique descendante des segments « cyber ». Corpus n°1	205
Figure 7 – Chi 2 – Formes les plus représentatives de chaque classe. Corpus n°1	205
Figure 9 – Analyse de similitude en l’absence des termes « cyber ». Corpus n°1	206
Figure 10 – Analyse de similitude des termes « cyber ». Corpus n°1	207
Figure 11 – Descriptif du corpus d’étude « Cyber JO UE 2001–2016 ».....	210
Figure 12 – Recensement des occurrences des termes « cyber ». Corpus n°2	212
Figure 13 – Chi2 – Classification hiérarchique descendante des segments « cyber ». Corpus n°2	214
Figure 14 – Chi 2 – Formes les plus représentatives de chaque classe. Corpus n°2	214
Figure 15 – Analyse de similitude en l’absence des termes « cyber ». Corpus n°2	215
Figure 16 – Analyse de similitude à partir des termes « cyber ». Corpus n°2.....	216
Figure 17 – Descriptif du corpus d’étude « Cyber DOC ONU 2001–2016 ».....	218
Figure 18 – Recensement des occurrences des termes « cyber ». Corpus n°3	220
Figure 19 – Chi2 – Classification hiérarchique descendante des segments « cyber ». Corpus n°3	222

Figure 20 – Chi2 – Formes les plus représentatives de chaque classe. Corpus n°3	222
Figure 21 – Analyse de similitude en l'absence des termes « cyber ». Corpus n°3	223
Figure 22 – Analyse de similitude à partir des termes « cyber ». Corpus n°3.....	224
Figure 23 – Calculs des occurrences – groupes de substantifs principaux par corpus (en nombres et pourcentages)	226
Figure 24 – Calculs des occurrences – Résultats totaux par année et par corpus (en nombre et en pourcentages)	227
Figures 25 et 26 – Projections des résultats de calcul des occurrences en pourcentages des résultats exprimés par corpus et en résultats exprimés par corpus	228
Figure 27 – Classifications hiérarchiques descendantes, substantifs les plus représentatifs de chaque classe.....	229
Figure 28 – Synthèse des analyses de similitudes sur les corpus 1, 2 et 3.....	230
Figure 29 – Descriptif du corpus d'étude « Cyber Factiva FR 2001–2016 ».....	232
Figure 30 – Recensement des occurrences des termes « cyber ». Corpus n°4	233
Figure 31 – Chi2 – Classification hiérarchique descendante des segments « cyber ». Corpus n°4	235
Figure 32 – Chi2 – Formes les plus représentatives de chaque classe (en chi2). Corpus n°4	235
Figure 33 – Analyse de similitude en l'absence des termes « cyber ». Corpus n°4	236
Figure 34 – Analyse de similitude à partir des termes « cyber ». Corpus n°4.....	237
Figure 35 – Descriptif du corpus d'étude <u>« Cyber Google News GnOSIE FR 2001–2016 ».</u>	239
Figure 36 – Recensement des occurrences des termes « cyber ». Corpus n°5	241
Figure 37 – Chi2 – Classification hiérarchique descendante des segments « cyber ». Corpus n°5	243
Figure 38 – Chi2 – Formes les plus représentatives de chaque classe (en chi2). Corpus n°5	243
Figure 39 – Analyse de similitude en l'absence des termes « cyber ». Corpus n°5	244
Figure 40 – Analyse de similitude à partir des termes « cyber ». Corpus n°5.....	245

Introduction générale

« L'information est pouvoir, et la technologie moderne de l'information propage celle-ci plus largement que jamais auparavant dans l'histoire. »

Joseph S. NYE¹

¹ Phrase extraite du chapeau du chapitre 1 « The Changing nature of power » de l'ouvrage: NYE Joseph S. *Soft Power: The Means To Success In World Politics*, Hachette UK, 28 avr. 2009, 208 p.

A la lecture de ces quelques mots, le précepte selon lequel l'information signifie pouvoir pourrait sembler nouveau. Il n'en est rien. En effet, si le mot « information » est assez récent, l'idée que dans une forme de connaissance réside une forme de pouvoir n'est pas nouvelle et traduit une préoccupation très ancienne². Toutefois en 2009, Joseph S. Nye insiste sur deux éléments importants : d'une part, la technologie de l'information et d'autre part, une logique de diffusion. Ces deux éléments décrivent la diffusion d'un corpus technologique de pointe construit autour de l'informatique à moindre coût vers une population massive qui renforcerait le pouvoir procuré par l'information. Si les préoccupations autour de l'information sont anciennes de même que les mouvements d'institutionnalisation de celle-ci, l'information automatisée prend depuis quelques années une forme nouvelle en étant associée à l'idée de sécurité grâce au terme « cyberespace » et à ses dérivés.

Forgé et développé par l'auteur de science-fiction William Gibson à partir de 1982³, le terme cyberespace est depuis passé dans le langage et a produit de nombreux dérivés composés autour du préfixe « cyber- ». En quelques années, le préfixe « cyber » est devenu le label servant à qualifier une série de mesures, de plans, de feuilles de route, d'accords [...] qui renvoient au final tous vers la même idée fixe : l'information doit être comprise comme un objet de sécurité. Autrement dit, non seulement la protection de l'information constitue un enjeu pour l'acteur considéré, mais ce dernier associe cet enjeu à l'idée de sa propre sécurité.

Cette association contribue ainsi à faire passer le cyberespace d'un phénomène hallucinatoire consenti et quotidien qui incarne la mémoire de l'humain à travers l'outil informatique, à une véritable idéologie sécuritaire tournée vers l'information et organisée autour de plusieurs registres discursifs allant du normatif à la technique en passant par l'idéalisme et le catastrophisme.

² Dans l'un des plus anciens traités de stratégie militaire *L'Art de la Guerre* de Sun Tzu (dont l'écriture est située entre le VIème et le Vème siècle avant notre ère et qui est introduit en Europe en 1772) les connaissances sont la base même de la guerre. « Les connaissances que je viens d'indiquer vous permettront de discerner, parmi les princes qui gouvernent le monde, celui qui a le plus de doctrine et de vertus ; vous connaîtrez les grands généraux qui peuvent se trouver dans les différents royaumes, de sorte que vous pourrez conjecturer assez sûrement quel est celui des deux antagonistes qui doit l'emporter ; et si vous devez entrer vous-même en lice, vous pourrez raisonnablement vous flatter de devenir victorieux. » « Ces mêmes connaissances vous feront prévoir les moments les plus favorables, le temps et l'espace étant conjugués, pour ordonner le mouvement des troupes et les itinéraires qu'elles devront suivre, et dont vous réglerez à propos toutes les marches. » SUN TZU, « I – De l'évaluation » in. *L'Art de la Guerre*, Paris, Éditions Flammarion, collection « Champs », 1978.

³ Voir. Chapitre liminaire.

Après un succès littéraire et culturel, cette seconde mode sécuritaire du cyberspace prend sa source dans une période de quelques années entre 2005 et 2008. Un récit est souvent décrit comme une prise de conscience grâce à un élément déclencheur officiel à ce mouvement (les événements estoniens de 2007). Ce récit épisodique se doit d'être restitué dans une période plus large 2005-2008 qui aura vu tout à la fois consacrer la question de la gouvernance d'Internet, naître le smartphone et les sites de « réseaux sociaux » tels *Twitter* ou encore le site *Wikileaks*, et au terme de plusieurs évènements verra l'ensemble du spectre des menaces se réaliser jusqu'à consacrer l'idée de lutte informatique.

Au-delà d'un choix d'instruments, de collecte de données et d'un terrain, cette thèse est la restitution d'un projet de recherche. Lancé fin 2012, ce projet s'est déroulé sur plusieurs années entre la Bretagne, la région parisienne et la Provence. Il sera passé par de nombreuses rencontres, étapes et expériences qui lui auront donné cette forme. Mais pour un jeune étudiant breton en 2007, cet intérêt pour les usages conflictuels de la technologie a également commencé avec le récit des évènements estoniens.

Des récits « officiels » à dépasser : le réveil « cyber » de la « nuit de bronze » (Estonie, avril-mai 2007)

Au début des années 2000, la situation économique de l'Estonie est favorable, malgré une forte inflation. La volonté politique de l'État a entraîné un rapprochement avec l'Union Européenne et une volonté d'intégrer la zone euro, ce que l'État finira par accomplir en 2011. En parallèle de ce processus l'Estonie est également membre de l'OTAN et de l'espace nordique⁴. Ce couple entre une volonté d'intégration régionale et un développement économique forts est marqué par une augmentation relative de la dette (4,11 % du PIB en 2006, un des taux les plus faibles en Europe) la réduction du chômage, les augmentations des importations et des exportations, le retour d'une balance commerciale excédentaire en 2006 et une croissance record de 11,4 % la même année. Ce développement économique s'appuyait essentiellement sur l'immobilier et sur le secteur financier mais reposait également sur de forts

⁴ Sur la perception de l'Estonie de la Russie, de l'Europe, des États-Unis et de l'espace nordique, voir l'article dans le numéro de la revue Anatoli de 2011 sur les représentations du monde dans l'espace postsoviétique dirigés par Kazancigil Ali et Prévelakis Georges : KESA Katerina, « Estonie : une représentation du monde singulière, postsoviétique et européenne », *Anatoli*, n°2, 2011, pp. 63-77

investissements étrangers (européens et russes notamment)⁵. Depuis la fin de la Guerre froide, les relations entre la République estonienne et la Fédération de Russie ont souvent été tendues. En dehors des raisons historiques, ces tensions sont principalement dues et demeurent du fait que coexistent en Estonie deux populations principales : l'une, majoritaire (69% de la population), a pour langue maternelle l'estonien (langue fennique), l'autre, minorité la plus importante (30%) a pour langue maternelle le russe (langue slave orientale).⁶

Depuis 2005, ces tensions communautaires se cristallisent autour d'un monument aux morts soviétique consacrés aux soldats tombés lors de la Seconde Guerre mondiale. Composé d'un mur de dolomite et d'une statue de bronze figurant un soldat le regard penché en signe de deuil, ce monument fut inauguré en 1947 dans un quartier du centre de Tallinn à proximité de tombes de guerre et alors intitulé « Monuments aux libérateurs de Tallinn ». Toutefois, c'est le nom de « soldat de bronze » qui demeurera. Les tensions communautaires autour de cette statue sont le fruit de deux représentations de celle-ci. Pour la communauté russophone, elle représentait tout à la fois une forme de résistance face à l'Allemagne nazie durant la Seconde Guerre mondiale ainsi qu'une reconnaissance des droits de la minorité en Estonie. A l'inverse pour la majorité, celle-ci symbolisait l'occupation de l'URSS et de répression durant la Guerre froide. Début 2007, ce conflit pris de l'ampleur par les agissements des nationalistes estoniens. Soucieux de taire ces tensions, le gouvernement prit une loi « sur la protection des sépultures militaires » afin d'entériner l'idée d'un déplacement de la statue dans un cimetière militaire. Le nouveau gouvernement issu des élections de mars 2007 a affirmé vouloir mettre à exécution ce projet. Ce thème du déplacement de la statue avait d'ailleurs été l'un des thèmes de la campagne électorale. De là, entre le 26 et le 28 avril 2007 s'en suivirent les émeutes les plus violentes que l'Estonie n'avait jamais connues depuis son indépendance en 1917. Alors qu'une tente était érigée pour démonter le monument, un millier de manifestants russophones sont intervenus pour défendre ce dernier entraînant une confrontation avec les forces de l'ordre, une émeute puis des pillages dans le centre-ville occasionnant d'importants dégâts matériels. C'est la « nuit de bronze ». Alors que le gouvernement déplace la statue le lendemain en catastrophe, de nouvelles émeutes éclatent le

⁵ Pour une analyse plus complète du contexte entourant l'événement, voir notamment l'article : CHALVIN Antoine, « L'ombre du soldat de bronze », *Le Courrier des pays de l'Est*, 2007/4 (n° 1062).

⁶ Voir notamment : DAUTANCOURT Vincent. « Les minorités russes en Estonie : unité et diversification », *Hérodote*, vol. 128, no. 1, 2008, pp. 73-85, ainsi que l'ouvrage CHAMONNOIS Suzanne et LABRIOLLE François, *L'Estonie : des Estes aux Estoniens*, Paris, Karthala (Méridiens), 1997, 277 p.

27 et le 28 avril. Le bilan humain est lourd, outre les arrestations, ces événements ont engendré un total de 150 blessés ainsi qu'un décès : un manifestant en a tué un autre à l'arme blanche.

La violence de la réaction russe a toutefois permis au gouvernement de ne pas engager sa responsabilité politique concernant la gestion de cette crise du soldat de bronze. En effet, la Russie a condamné officiellement ce déplacement de statue. Des sanctions économiques ont été prises. Des entreprises russes ont appelé au boycott des produits estoniens. Tandis que des militants pro-russes assiégeaient l'ambassade estonienne à Moscou, tentant même d'en agresser physiquement l'ambassadrice, l'Estonie recevait des « monuments vivants », des jeunes femmes et hommes allant en uniforme se tenir là où le monument était auparavant situé. Néanmoins, la conséquence qui nous intéresse le plus ici se passe sur Internet.

En effet, à partir du 27 avril 2007, une vague de cyberattaques sans précédent a été lancée sur l'ensemble des sites institutionnels estoniens. Ces attaques de type déni de service (*DDoS, Distributed Deny of Service*) sont arrivées depuis tous les coins du globe (environ 60 États concernés). Ces attaques ont duré 3 semaines atteignant leur paroxysme en mai où elles touchèrent le site de la plus grande banque estonienne (dans un contexte où 90% des transactions bancaires de l'État se réalisaient par Internet)⁷. Les attaques n'ont jamais pu être formellement attribuées à l'État russe. Le pirate pro-russe finalement arrêté a d'ailleurs nié l'implication des autorités russes dans sa démarche. Cela n'a pas empêché l'Estonie, puis l'Otan de se préoccuper du comportement supposé de l'État russe et favoriser une représentation de celui-ci comme une menace.

Une mise en récit insérée dans une succession d'évènements entre 2005 et 2008 : de la gouvernance d'Internet à la lutte informatique.

Néanmoins, si l'exemple estonien est souvent cité et qu'il aura servi à justifier certaines mesures exceptionnelles concernant la sécurité de l'information, il doit être resitué dans un temps plus large qui intègre plusieurs évènements dans une forme de prise de

⁷ L'Estonie est l'un des États les plus technologiquement développé d'Europe. En 2004, la population de l'Estonie comptait 45% d'internautes quand la France n'atteignait pas les 40%. Par ailleurs, le parlement estonien garantit l'accès à Internet comme étant un droit constitutionnel. Le gouvernement estonien a renoncé totalement au papier pour ses réunions de cabinet, il travaille via réseau Internet interne accessible aux citoyens. A cette époque, en Estonie avec un téléphone portable (avant l'avènement des smartphones) le citoyen pouvait déjà payer sa place de stationnement en ville, réservé une place de théâtre, acheter des tickets de loterie...

conscience de l'enjeu de la sécurité de l'information de manière plus large. L'idée de première importance qui émerge en 2005 est celle de la gouvernance d'Internet. Le Sommet Mondial sur la Société de l'Information, organisé par l'Union Internationale des Télécommunications (UIT)⁸. A l'issue de la première phase, à Genève, en décembre 2003, les États membres des Nations unies avaient adopté à l'unanimité un texte plaidant pour une gestion d'internet « multilatérale, transparente et démocratique, avec la pleine participation des États, du secteur privé, de la société civile et des organisations internationales ». La seconde phase qui s'est déroulée à Tunis, en novembre 2005, est venue concrétiser cette volonté avec la décision de mettre en place, en 2006, la naissance du forum de la gouvernance de l'Internet qui a pour but d'instaurer et faciliter le dialogue autour des différentes parties prenant part au jeu de ladite gouvernance⁹.

Sur la période 2005 – 2008, Internet lui-même évolue d'une part en termes de diffusion et de contenu. D'une part, le nombre d'internaute s'accroît de manière significative : en 2005, Internet passe la barre symbolique du milliard d'utilisateurs pour atteindre un milliard et demi en 2008¹⁰. En termes de contenu, la période 2005-2008 représente également un pic de popularité des réseaux sociaux (*Facebook, Twitter, MySpace...*) ainsi que les débuts du site *Wikileaks* qui offre à la fois le dévoilement d'un certain nombre de documents confidentiels ainsi qu'un nouvel espace de parole pour les lanceurs d'alerte sur lesquels nous aurons l'occasion de revenir. Du point de vue des incidents, outre les fuites de documents et les événements estoniens, la période aura constitué des années noires. Dès janvier 2007, c'est d'abord le cheval de Troie¹¹ *Storm Worm* qui fait des ravages dans les courriels. Le 6 février

⁸ UIT : La plus ancienne organisation intergouvernementale technique de coordination, puisqu'elle a été créée sous le nom d'Union internationale du télégraphe en 1865. Le développement du téléphone aidant, elle adopte son nom actuel en 1932 et se voit rattachée directement aux Nations unies en 1947.

⁹ Son mandat regroupe précisément la politique publique globale au niveau local et intergouvernemental en relation avec la gouvernance de l'Internet et la neutralité des réseaux. Ainsi que l'utilisation des compétences des parties universitaires, scientifiques et techniques, la réduction de la « fracture numérique mondiale », dans les principes de la transparence et du respect des principes du Sommet Mondial de la Société de l'Information. Pour une lecture critique de cet événement, voir notamment : LE FLOCHE Guillaume. « Le sommet mondial de Tunis sur la société de l'information », *Annuaire français de droit international*, volume 51, 2005. pp. 464-486.

¹⁰ Selon les chiffres de l'IUT (*ICT Facts and Figures*)

¹¹ Le « cheval de Troie » est une grande catégorie de logiciels malveillants ou *malware*, dont la spécificité commune réside dans la légitimité apparente d'un logiciel qui dissimule un parasite informatique.

2007, des attaques ont lieu sur quatre des 13 serveurs racine DNS¹². Les attaques sont stoppées avant de provoquer des dégâts trop importants bien que deux d'entre-deux aient été touchés de manière importante. Le 30 janvier 2008 ce sont des câbles sous-marins dans la Méditerranée (SEA-ME-WE 4 et FLAG) dont la coupure a entraîné des pannes d'Internet au proche Orient ainsi qu'en Inde. Le 2 février 2008, le câble FALCON fut à son tour endommagé dans le Golfe Persique à Dubaï. Ces coupures de câbles entraînèrent une perte d'échange entre l'Europe et les régions concernées allant de 60 à 80% en fonction des estimations. 2008 est enfin l'année où débutent les premières estimations de perte de données personnelles des clients d'opérateurs téléphoniques (Verizon notamment avec des pertes chiffrées en millions de données utilisateurs).

Par ailleurs, l'année 2008 connut un évènement militaire où l'utilisation de l'informatique couplée avec des moyens militaires posa à nouveau question à propos de la Russie : il s'agit de la Deuxième guerre d'Ossétie du Sud. Dans la nuit du 7 au 8 août 2008, la Géorgie donnait l'assaut en Ossétie du Sud. En moins de vingt-quatre heures, les unités blindées de la Russie, stationnées en république autonome d'Ossétie du Nord, sont arrivées sur le terrain. Mais dans un délai de 6h à 8h avant l'arrivée des chars, les sites sensibles du gouvernement géorgiens furent la cible d'attaques informatiques de type DDoS¹³ qui ont paralysées un certain nombre de sites et de services gouvernementaux. La surenchère médiatique qui s'en suivit ne fut pas sans rappeler celle qui avait entourée l'Estonie en 2007. Les deux affaires furent associées dans un discours contre la Russie assez poussé oubliant que de nombreux sites russes avaient eux-mêmes fait l'objet d'attaques similaires. Les comparaisons s'établissent rapidement avec la guerre de l'information des années 90 et la Première Guerre du Golfe, à la différence près du média puisque ce n'est plus la télévision qui est la plus mobilisée mais Internet... Cette image de la cyberguerre « venue du froid » ou « cyberguerre froide »¹⁴, sera rapidement ajoutée des premiers développements sur la Chine durant l'été 2008 avec les Jeux olympiques d'été qui ont été à la fois une démonstration d'une couverture Internet massive grâce à un accord entre la plateforme *Youtube* et le Comité International

¹² Le *Domain Name System* (DNS, système de noms de domaine) est un service permettant de traduire un nom de domaine en informations de plusieurs types, notamment en adresses IP. Le terme a émergé en 1983. Bien que les serveurs soient situés à plusieurs endroits sur la planète, l'administration est assurée par l'*Internet Corporation for Assigned Names and Numbers* (ICANN), société de droit californien à but non lucratif.

¹³ Cf. Supra.

¹⁴ En référence à de nombreux commentaires de presse parus à l'époque

Olympique, ainsi qu'une nouvelle controverse autour de la censure, de la surveillance et de la délations des usages d'Internet employant des moyens policiers colossaux. Le libre accès à Internet était déjà en question depuis mars 2008 avec les troubles politiques au Tibet. Des journalistes présents sur place ont pu constater une forme de censure de nombreux médias d'informations et de sites d'Organisations non-gouvernementales¹⁵. Cette période voit enfin se structurer tout un ensemble de concepts et d'institutions qui formeront le socle normatif de la cyberdéfense et plus largement de la cybersécurité. Aux États-Unis, en 2007 c'est la naissance de l'*Air force Cybercommand*¹⁶. En 2008, en France, le *Livre blanc sur la défense et la sécurité nationale* créait le concept de lutte informatique défensive et offensive. Toujours en 2008, l'OTAN crée également le *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) à Tallinn avec pour mission l'amélioration des capacités, de la coopération et du partage d'information entre les pays membres et partenaires de l'OTAN dans les « nouveaux » domaines de la cybersécurité ou de la cyberdéfense entre autres par des actions de formation et de recherche et développement. Cette brique de départ viendra soutenir l'ensemble du foisonnement institutionnel et normatif qui suivit cette période à la fois au niveau privé, au niveau étatique et au niveau international.

Problématique de la recherche.

Cette recherche a été entamée sur un questionnement de départ : « Du fait de ses nouveaux usages pour qualifier des relations interétatiques bilatérales, puis des enjeux multilatéraux, le cyberespace peut-il être regardé comme un objet des Relations Internationales ? ». En apparence simple, cette question a soulevé en elle-même de nombreuses interrogations disciplinaires¹⁷. L'ambition de ce travail de thèse est de comprendre la relation entre un phénomène du langage et sa réception à travers l'idée qu'il représente par le prisme de la Science politique et des Relations Internationales ; puis, de renverser la logique de cette compréhension en éclairant l'apport de cette relation dans ledit champ académique. Cette question de savoir si le cyberespace peut être qualifié d'objet des Relations Internationales induit un premier travail réflexif autour du champ lui-même. Au sein

¹⁵ A ce sujet voir notamment l'ouvrage de Séverine Arsène tiré de sa thèse en Science Politique soutenue à l'IEP de Paris en 2009 : ARSENE Séverine, *Internet et politique en Chine : les contours normatifs de la contestation*, Karthala, Paris, 2011, 420 p.

¹⁶ Lequel ne sera finalement pas activé et verra sa compétence transférée à l'*US Cybercommand* en 2008, qui lui sera activé en 2011.

¹⁷ Lesquelles seront résumées au sein du chapitre liminaire.

des Relations Internationales, une branche particulière s'intéresse au recensement et à l'analyse de ces différents débats : il s'agit des Théories des Relations Internationales. S'interroger sur la nature d'objet des Relations Internationales conduit à questionner de façon croisée la notion (cyberespace) et les débats théoriques qui structurent le champ, en adoptant une problématique double : Comment les Théories des Relations Internationales peuvent-elles comprendre le cyberespace ? Que peut apporter le cyberespace à la compréhension et à l'étude des Relations Internationales ?

Ce double questionnement suppose l'identification des questions que pose le cyberespace aux Relations Internationales. Identifier ces questions implique de définir tout d'abord : Qu'est-ce que le cyberespace ? Comment comprendre la prolifération de formes et de sens dont il fait l'objet ? Quelles représentations sont véhiculées par les usages de ces substantifs ? Et quels modèles théoriques peuvent être employés pour décrire le monde à partir de ces mêmes représentations ? L'hypothèse principale de cette recherche est construite autour du postulat que le cyberespace et ses termes dérivés participent d'un même phénomène discursif. La possibilité d'objets communs existant au-delà du seul phénomène linguistique dans le champ des Relations Internationales permettra d'une part de mesurer l'effet de la notion sur la compréhension de ces objets et donc les apports à l'étude de la dimension internationale du Politique.

L'un des intérêts premiers de cette approche consiste à déconstruire une illusoire technicité homogène et connotée d'un langage « cyber » souvent nominaliste. La plupart des ouvrages académiques tendent à réifier cette idée et les représentations qu'elle implique en considérant l'ensemble comme un système animé de préceptes figés garantis par une « scientificité » du propos et en focalisant leur regard sur ses aspects positifs ou négatifs. C'est-à-dire, sous formes de visions d'un futur représentant une opportunité sous les atours d'un nouvel « âge d'or numérique » ou le retour à l'état de nature « hobbesien » sous couvert du virtuel. L'analyse de ce discours comme un marqueur idéologique permet d'accéder à un angle d'approche à la frontière d'une prise de conscience autour de l'information, laquelle ne s'inscrit pas tant dans une vision du futur que dans la compréhension d'une forme de complexité tout à fait actuelle.

Selon les résultats de cette recherche, le terme « cyberespace », les termes dérivés et le préfixe « cyber » sont des marqueurs d'un discours à vocation de sécurité ayant pour objet

l'information. Ce discours mobilise l'espace fictif décrit comme la représentation d'une réalité sociotechnique complexe où prédominent avant tout des idées de menaces et de vulnérabilités : criminalité, terrorisme, sabotages, vols de données, violation des libertés des individus... La prise en compte de l'information comme enjeu de sécurité par l'acteur répond à une forme d'incertitude que les représentations du cyberspace participent à renforcer. Celle-ci vient questionner le paradigme de l'État régional comme unité fondamentale du système international, au profit d'une conception atomiste où l'État devient un « réseau social complexe » composé de divers acteurs moindres entretenant des rapports réductibles à des échanges d'information... La pluralité des acteurs en termes de natures, de nombres et d'inégalité ont déjà fait l'objet de plusieurs définitions et forment le socle de nombreux débats ontologiques. Envisagée à l'aune du réseau, cette pluralité doit être comprise comme un objet complexe nécessairement multiscalaire où les flux d'information (automatisés ou non) permettent d'identifier les relations construites entre des acteurs asymétriques, de toute nature et interdépendants, faisant du cyberspace un outil conceptuel transversal qui permet de fournir un point de vue sur la relation entre les différents niveaux d'organisation du Politique.

Architecture de la thèse.

En début de manuscrit, le chapitre liminaire est destiné à exposer l'approche épistémologique et méthodologique retenue dans ce travail de recherche. Ce chapitre met en avant la construction intellectuelle destinée à saisir l'objet « cyberspace » autour de deux volets : les Théories des Relations Internationales et de l'étude du discours.

Sur le premier ensemble, cette thèse fait le choix d'une combinaison pragmatique entre plusieurs théories des Relations Internationales pour saisir un objet politique. Parmi, ces théories la porte d'entrée sera constituée par les théories de la sécurité qui permettront à l'objet « cyberspace » d'être compris comme un objet politique.

Sur le deuxième ensemble, la thèse fera cette fois-ci le choix d'une épistémologie construite sur le concept de champ sémantique qui permettra de mettre en avant les circulations de l'objet d'étude entre les domaines littéraire, politique et scientifique. A partir de ce socle épistémologique, le chapitre liminaire mettra en relief une approche phénoménologique plurielle du cyberspace qui aura pour vocation de le déconstruire et de questionner son rapport à la technique, aux sciences et aux normes à l'aide de plusieurs outils de collecte de données. L'ensemble de ce travail s'inscrira dans une démarche abductive. Le

chapitre liminaire détaillera enfin les aspects pratiques de la recherche : l’engagement dans et par le terrain ainsi que les contraintes du projet de recherche.

Après avoir détaillé les éléments théoriques et pratiques du processus de recherche mis en œuvre, le manuscrit abordera l’exposé et la discussion des résultats de ladite recherche. L’ensemble du manuscrit est divisé en deux parties.

La première partie du manuscrit est consacrée à l’étude du phénomène que constitue l’utilisation du cyberespace et de ses termes dérivés. Découpée en trois chapitres numérotés de 1 à 3, cette partie vise à rendre compte des résultats de l’approche phénoménologique plurielle décrite dans le chapitre liminaire. Plus précisément, elle cherche à dépasser le problème de l’impossible définition technique du cyberespace en opérant un renversement du point de vue. Lequel n’est plus construit sur le contenu technique de la notion, mais sur l’évolution de son contenu idéal.

Le premier chapitre remet en question le rapport à la technique du phénomène analysé à travers la création du cyberespace dans la littérature. Dans un premier temps, abordée de façon factuelle, cette création sera contextualisée de façon à questionner ses héritages, les confusions qui entourent la notion et de critiquer son rapport à la technique.

Le deuxième chapitre, quant-à-lui, analysera l’impact normatif du phénomène linguistique « cyber » à travers l’analyse logométrique de l’utilisation des termes dérivées du cyberespace en français entre 2001 et 2016 dans les journaux officiels de la République française (Corpus 1) et l’Union Européenne (Corpus 2), ainsi que le système de documentation de l’Organisation des Nations Unis (Corpus 3). Ces trois corpus seront comparés à deux corpus supplémentaires basés sur les publications en français dans la presse à partir des bases de données de Factiva (Corpus 4) et Google (Corpus 5).

Le troisième chapitre a but de franchir une étape supplémentaire en évoquant l’appropriation sécuritaire du cyberespace dans un ensemble de discours labellisé par un marqueur linguistique « cyber » traduisant une préoccupation de nature régaliennes autour de la sécurité de l’information. Ce chapitre visera à évoquer la communauté des locuteurs de ces discours et d’aborder leur capacité d’influence à travers les concepts de communautés discursives et épistémiques. Cette communauté particulière constitue le terrain de la présente recherche.

La seconde partie du manuscrit repose la combinaison pragmatique des théories destinées à fournir l'explication en Relations Internationales du phénomène analysé. Elle est également découpée en deux chapitres numérotés cette fois-ci de 4 à 5. Cette partie interrogera l'agentivité des Relations Internationales et l'asymétrie des relations entre les acteurs, mais elle sera également l'occasion de mettre en relief le questionnement majeur de l'ensemble des travaux quels que soit leur courant et qui est celle de la place du déterminisme technique dans les relations internationales. Ou plus précisément, il s'agira pour la plupart des auteurs de décrire l'interdépendance de la politique internationale et du changement technologique.

Partant des données recueillies, le quatrième chapitre traduira le phénomène du langage dans les théories de la sécurité. Ce chapitre se focalisera sur les approches discursives de la sécurité et en particulier la sécurisation qui sera complétée de façon plus large par les Théories des Relations Internationales en examinant les recherches sur la sécurité de l'information ou d'autres débats notamment les recherches sur la gouvernance, le développement économique, les régimes autoritaires, et la société civile globale qui forment les autres problématiques liées à la réception de la sécurité de l'information dans les Relations Internationales.

Le cinquième chapitre et dernier comprend l'inventaire des questions théoriques qui émergent du quatrième chapitre et de mobiliser des théories qui proposeront une réponse. L'idée générale que l'acteur régional demeure le cadre de référence en mobilisant les théories « cyberpolitiques ». Dans un second temps, le chapitre s'appuiera notamment sur l'idée de réseau en mobilisant un développement sur l'application à la sécurité de la sociologie de la traduction et en particulier la théorie de l'acteur-réseau (*Actor-Network theory*).

Chapitre liminaire – Stratégie, méthode et conduite de la recherche.

« [...] , la méthode réside en un détour de la pensée pour passer d'un problème à sa solution, d'une question à sa réponse. La démarche méthodique ne va pas directement à la solution. Elle remplace la question par une autre : comment convient-il de s'y prendre pour accéder à la bonne réponse ? C'est que souvent la vérité se cache et l'esprit se heurte à un mur quand il cherche à la saisir immédiatement. La seule chance de succès est alors de réfléchir sur la question elle-même en vue de déterminer le traitement qu'elle appelle »

François GRUA¹⁸

Cette recherche doctorale a débuté sur la base d'une intuition : la conviction que l'emploi de la notion de cyberespace et son insertion dans le vaste domaine des Relations Internationales repose sur des pseudo-évidences. Ce point de départ implique une forte dimension discursive qui fait que les contours exacts et le contenu de la notion ne peuvent pas être définis avec précision sans mener un travail réflexif *a priori*. Notre question de départ impliquait ainsi une défiance particulière à l'égard des « idées reçues » sur le cyberespace mais aussi à l'égard des instruments et des conceptions employés pour l'analyser. Cette posture devrait conditionner les grandes orientations et les options méthodologiques du projet. L'actualité riche et la vitesse d'évolution du traitement sujet, présent dans les médias et la vie publique, ont entraîné une nécessité de rendre l'actualité intelligible et de produire une recherche qui puisse rendre compte de la complexité de l'objet en tenant compte de l'actualité internationale, les changements de postures de l'acteur régional¹⁹ et les développements progressifs du champ numérique. Cette démarche réflexive induite par l'objet de la recherche et ses évolutions a permis de construire notre grille d'analyse. La stratégie de recherche²⁰ mise en place pour répondre à la problématique est fondée sur un raisonnement abductif consistant en un échange quotidien permanent entre théorie et observation empirique. Ce choix transversal interroge les relations entre la recherche et la théorie, la temporalité et l'échelle de

¹⁸ Première leçon tirée de la définition générale de la méthode François Grua dans son introduction à la méthode des études de droit. GRUA François et CAYROL Nicolas, *Méthode des études de droit*, Paris, Dalloz, 2^{ème} édition, 2011, 132 p (p. 1).

¹⁹ Par exemple, en France, le passage de la lutte informatique défensive (LID) comme seul choix consacré politiquement, à la reconnaissance d'une possibilité de recours à la lutte informatique offensive (LIO) affirmé dans le courant de l'année 2015.

²⁰ Cf. Figure 1

l’analyse retenues. Cette stratégie de réponse repose sur trois piliers interdépendants que sont les Relations Internationales, les études de sécurité et les analyses de discours. L’analyse du discours sert à dégager un phénomène de transformation de l’information en enjeu de sécurité. Cet enjeu traduit différents problèmes susceptibles d’appréhension par les Théories Relations Internationales envisagée de manière pluraliste dans la construction d’un texte explicatif idéal des enjeux propres à la sécurisation de l’information en Relations Internationales. Ce texte explicatif idéal fruit d’une approche « problem-driven » formera la base de la présente recherche et servira la présentation et la discussion de ses résultats.

Le but de ce chapitre liminaire est de rendre compte des choix opérés, de présenter les outils mis en place pour répondre à la problématique avec leurs limites et d’évoquer les difficultés rencontrées au cours de la recherche. Il vise d’abord à mettre en lumière la solution construite pour répondre à la problématique entre le cadre des Relations Internationales, des études de sécurité et des analyses de discours, ainsi que les différentes directions explorées et retenues. Elle restitue également la compréhension des ensembles théoriques mobilisés dans le cadre de cette recherche. Comme toute synthèse, celle-ci présente deux défauts majeurs : D’une part, elle n’a pas prétention à l’exhaustivité. D’autre part, elle mériterait sans doute bien des approfondissements. Cette stratégie de recherche reflète l’orientation générale de la démonstration, mais ne doit pas être comprise comme une stratégie d’information organisée uniquement autour de la collecte et de l’analyse des données. En effet, elle s’accompagne d’un mode de travail et de raisonnement itératif ainsi que d’éléments pratiques qui lui sont complémentaires. Cet ensemble ne forme pas le résultat proprement dit de cette recherche mais en constitue pourtant l’une des caractéristiques principales. Au-delà d’une double contrainte « objet/champ » propre à la problématique, la démarche globale de cette recherche l’inscrit en tant que mode de production d’un discours scientifique dans un domaine académique pluraliste : la Science Politique²¹. Elle procède d’ensembles disciplinaires hétérogènes. Ainsi, l’enjeu est double. Tout d’abord, la démarche de recherche doit apporter

²¹ Objet et source de controverse, cette appellation pose déjà question dans chacun de ses vocables qui la compose et dans leur association. Plus généralement, l’histoire de la discipline est rarement présentée par ses mutations, débats voire conflits. A ce sujet, voir par exemple, COMAN Ramona, CRESPY Amandine, LOUAULT Frédéric, MORIN Jean-Frédéric, PILET Jean-Benoit, HAUTE (VAN) Emilie, *Méthodes de la Science Politique*, Paris, De Boeck, 2016, 224 p. Ainsi que plus classiquement : FAVRE Pierre, « La connaissance politique comme savoir légitime et comme savoir éclaté. », *RFSP*, 1983, pp. 467-503. Cette question se pose pour tous les domaines associés à la Science Politique : Philosophie politique, Sociologie politique, Relations Internationales, dont chacune viendra également se poser la question de sa propre autonomie en tant que discipline.

une réponse au fait du pluralisme. Ensuite, elle doit former le cadre facilitant l'intégration des divers concepts²². D'une façon générale, cette recherche n'a pas pour vocation à soutenir la primauté d'une compréhension du réel sur une autre. Il en admet volontairement une nature subjective²³ et objective. Cette démarche repose sur une prémissse qui veut que toute réalité sociale se comprend comme le résultat d'interactions complexes visibles et invisibles, dans lequel la perception et donc la connaissance scientifique demeurent limitées. Cette connaissance doit donc se construire avec et au-delà la réalité observable. Elle admet l'étude scientifique dans une compréhension multi-causale et contextualisée du phénomène politique mais en relativisant les explications mono-causales et la portée prescriptive « universelle » desdites explications. En tant que telle, la réalité n'est pas déterminée seulement par des évènements, des perceptions, des valeurs et des discours, mais également par des structures et des rapports de pouvoir qui sont identifiables ou caractérisables par l'expérience ou/et les discours. Dans cette posture, le discours joue un double rôle en tant qu'objet en lui-même et en tant que vecteur de représentations d'autres phénomènes politiques. Trois éléments ressortent de cette posture : Par son activité, le chercheur exerce une influence sur la réalité observée. Cette réalité ne peut être comprise qu'à partir des objets de notre connaissance qui n'existent pas indépendamment de leur propre langage et de leur interprétation. Enfin, loin d'être déconnectés de la réalité, les objets théoriques et leurs déclinaisons sont donc les mieux à même de traduire d'admettre la complexité de cette réalité. La théorie permet de décrire les évènements, de les comprendre, mais aussi de prévoir et d'influencer ces évènements²⁴.

Section 1 – Théories des Relations Internationales : des paradigmes à la combinaison pragmatique.

Si l'étude de la politique internationale est ancienne, les Relations Internationales en tant que discipline académique sont souvent regardées comme « jeunes ». Au Royaume-Uni la discipline académique des Relations Internationales existe depuis 1919. Cette discipline s'est par la suite développée aux États-Unis après la Seconde Guerre mondiale. En France, les

²² Dans le cadre de cette thèse, c'est par exemple du cas de la notion linguistique de « cooccurrence ».

²³ A l'image d'une société construite et reproduite par les interactions entre les individus et qui suppose une co-construction intersubjective entre la structure et les agents. Voir : BERGER Peter et LUCKMANN Thomas, *La construction sociale de la réalité*, Paris, Armand Colin, 3^{ème} édition, 2012, 344 p.

²⁴ Ces deux derniers points sont souvent perçus comme une pierre d'achoppement des « internationalistes ».

historiographies de la discipline soulignent un rôle fondateur des travaux sociologiques de Raymond Aron²⁵. L'essor des Relations Internationales en France s'inscrit dans le champ de la Science Politique à partir des traditions historiques et juridiques. Cette construction reproduit de façon analogue la genèse laborieuse et les grandes divisions de la Science Politique un siècle auparavant. L'obstacle est d'abord intellectuel puisqu'une discipline doit obtenir un accord minimum sur les objets et les problématiques centrales à étudier. Il s'agit ensuite à un niveau institutionnel de développer des lieux et des supports propres à diffuser la discipline et à l'inscrire dans le temps. Et enfin, à un niveau social doit voir le jour une communauté savante avec dont le rôle est de légitimer et catalyser la discipline²⁶. Comme la Science Politique, les Relations Internationales semblent victimes de la division académique profonde entre la philosophie et la théorie politique, la sociologie et l'emprise du droit qui conditionne une approche normative et institutionnaliste du politique. Ainsi se pose la question de l'autonomie des Relations Internationales comme discipline et un certain sentiment d'illégitimité en France et face aux Relations Internationales mondiales notamment anglo-saxonnes.

L'article de Jörg Friedrichs consacré aux Relations Internationales en France²⁷ décrit une construction fondée sur l'histoire et la sociologie, en marge de la discipline anglo-saxonne. La contribution de l'histoire à la discipline se retrouve chez Pierre Renouvin et Jean-Baptiste Duroselle. L'apport de la sociologie s'exerce quant à lui en trois vagues : d'abord avec la sociologie compréhensive « weberienne » de Raymond Aron, puis avec la sociologie systémique de Marcel Merle et enfin avec la sociologie « a-théorique » portée notamment par Bertrand Badie²⁸. La sociologie des Relations Internationales constitue en France une

²⁵ Plus particulièrement, la réception de l'ouvrage *Paix et guerre entre les nations* dont la première édition a été publiée chez Calmann-Lévy en 1962. Toutefois les discussions commencent dès les années 50, avec la proposition d'une synthèse pour une étude historique des relations internationales de Jean-Baptiste Duroselle. DUROSELLE Jean-Baptiste, « L'étude des relations internationales. Objet, méthodes, perspectives », *Politique étrangère*, décembre 1952, pp 229 - 232.

²⁶ Voir les critères d'émergence dégagés par Pierre Favre. FAVRE Pierre, *Naissances de la Science Politique en France 1870-1914*, Paris, Fayard 1989, 331 p.

²⁷ FRIEDRICHS Jörg, « International Relations Theory in France ». *Journal of International Relations and Development*, janvier 2001, pp 118 - 137.

²⁸ Ces trois vagues sont également décrites par Dario Battistella dans les chapitres consacrés à la France dans son ouvrage, voir BATTISTELLA Dario (2003), *Théories des Relations Internationales*, 4^{ème} éd., Paris, Presses de Science Po, 2012, pp 689 – 722 et BATTISTELLA Dario, « La France » In. BALZACQ Thierry et RAMEL Frédéric, *Traité de Relations Internationales*, Paris, Presses de Science Po, 2013 pp 157 - 180.

approche majoritaire. A rebours des deux premières vagues, la troisième vague sociologique revendique sous la plume de Bertrand Badie, Marie-Claude Smouts, Guillaume Devin, une émancipation des Relations Internationales françaises par rapport à la discipline mondiale. Cette émancipation se fonde sur une conception des Relations Internationales comme la dimension internationale du politique qui est particulière par sa taille et sa complexité²⁹. La place des Théories des Relations Internationales y est limitée, notamment du fait d'une déconsidération critique au profit de l'objectif d'études empiriques et faisant la part belle au dialogue interdisciplinaire. Du point de vue des théories, cette sociologie peut être perçue comme une forme de transnationalisme implicite fondé sur les idées d'instabilité du système international et de crise de l'État³⁰ ³¹. De leur(s) côté(s), les théories des Relations Internationales, comprises comme « production d'approches savantes compétitives désireuses de rendre compte en des termes abstraits des principes conducteurs des interactions politiques qui se déroulent au-delà des territoires nationaux »³² sont décrites comme minoritaires. Ces approches supposent d'accepter un dialogue avec les développements des Relations Internationales anglo-saxonnes et notamment la pluralité des théories les modèles des débats.

A – Un contexte général non-consensuel et polysémique : théories et grands débats « inter-paradigmatiques ».

Sur une période symbolique d'un siècle depuis l'entre-deux-guerres, l'historiographie classique des Relations Internationales présente une construction disciplinaire autour de grands débats scientifiques. Au sein de la discipline, ces débats sont qualifiés de débats « inter-paradigmatiques » dans la mesure où ils procèdent traditionnellement de confrontations entre

²⁹ VERNANT Jacques, « Vers une sociologie des relations internationales », *Politique étrangère*, 1962.

³⁰ Du fait de l'existence chez Bertrand Badie, d'une théorie du « jeu triangulaire » impliquant États, acteurs transnationaux et communautés identitaires. Voir BATTISTELLA, *Théories des Relations Internationales*, op.cit. p 713.

³¹ D'autres formes de sociologie existent notamment la sociologie de Didier Bigo et de l'« école de Paris » dans les études de sécurité, sur laquelle nous reviendrons au moment d'évoquer ces dernières. Laquelle rejoint volontairement les débats épistémologiques du champ et donc s'inscrit dans la discipline à l'échelle internationale.

³² FRIEDRICH, op.cit. traduction de BATTISTELLA, 2012, op.cit. p. 689.

deux paradigmes³³ (et rarement plus). Ils participent plus largement à la formation d'un environnement concurrentiel et compétitif autour de la supériorité théorique bien que cette tendance soit à la baisse. En effet, dans ce modèle simplificateur, chacune des « écoles de pensée » de la discipline cherche à s'imposer face aux factions adverses (et l'une d'entre-elle en particulier). Cela implique une première étape qui est la définition de ces théories et de leur nombre³⁴. Ce goût des théories pose question : apprécier uniquement des faits ne serait-il pas préférable à la construction d'un dédale croissant de théories ? Autrement dit, quel est l'utilité de ces théories ?

En 1994, Fred Halliday³⁵ dégage un intérêt triple à cette question. Une théorie des Relations Internationales est intéressante car : d'une part, il y a besoin de préconceptions minimales pour pouvoir donner du sens à des faits. Ceux-ci ne suffisent pas quel que soit le domaine académique ou non³⁶. D'autre part, les faits mêmes acceptés comme vrais sont objet d'interprétation³⁷. Enfin, aucune activité sociale ne peut se contenter des faits et faire abstraction des questions morales qu'elle induit, morale qui échappe au domaine des faits. Si chacune des écoles, traditions, tendances, perspectives [...] dispose de son propre paradigme intrinsèque³⁸, les Relations Internationales ne disposent d'aucun paradigme propre car il n'y

³³ Introduit par les travaux de Thomas Kuhn en 1962 (voir en français : KUHN Thomas, *La Structure des révolutions scientifiques*, Paris, Flammarion, coll. « Champs-Sciences », 2008, 286 p.), le paradigme fait l'objet d'appropriation et de conceptualisations diverses voire d'une surabondance d'utilisations. A partir de la seconde édition de son ouvrage en 1970, Kuhn identifie deux sens globaux parmi les acceptations du paradigme : d'une part, en tant que croyance partagée par une communauté scientifique ; d'autre part, en tant que modèle théorique qui implique une orientation de la recherche et des méthodes pour résoudre des problèmes. Le paradigme sera compris comme une conception du monde acceptée par la majorité des membres d'une communauté et qui détermine pour partie les postulats auquel le chercheur à recours. Sur la polysémie qui entoure le terme paradigme, voir notamment la critique des travaux de Thomas Kuhn par Margaret Masterman et les 21 sens du mot : MASTERMAN Margaret, « The Nature of a Paradigm », In. LAKATOS Imre et MUSGRAVE Alan (dir.), *Criticism and the Growth of Knowledge*, New York, Cambridge University Press, 1970 pp. 61 - 65.

³⁴ Voir notamment la question soulevée par l'article : KORANY Bahgat. « Un, deux, ou quatre... : Les écoles de relations internationales ». *Études internationales* 15, n° 4, décembre 1984, pp. 699–723. L'article s'attarde à l'époque, sur le libéralisme, le réalisme, le bélaviorisme, le marxisme et le néo-marxisme avec l'école de la dépendance.

³⁵ Voir le chapitre « *Theories in Contention* » (pp 23 à 47) : HALLIDAY Fred, *Rethinking International Relations*, Vancouver, University of British Columbia Press, 1994, 304 p.

³⁶ « The facts are myriad and do not speak for themselves » (« Les faits sont une myriade et ne parlent pas pour eux-mêmes »), Ibid p. 25,

³⁷ Fred Halliday prend l'exemple du débat sur les « leçons de 1930 » qui ne concerne pas les événements de 1930 mais la manière de les interpréter.

³⁸ L'idée inter-paradigmatique procède ici d'une forme d'abus car elle ne pourrait s'appliquer qu'au débat ontologique, ou troisième débat, consacré aux acteurs. Inter-paradigmatique suggère qu'il y a deux paradigmes concurrents ce qui dépasse la conception de Kuhn pour qui le paradigme équivaut à une science normale.

aurait pas de conception du monde qui emporte la majorité des suffrages et finalement peu de nouvelles théories qui viennent « remplacer » les anciennes³⁹. La plupart des théories viennent en effet d'ajouter de façon cumulative rendant la lecture de l'ensemble peu évidente. Toutefois, le réalisme est souvent considéré comme la théorie dominante dans le champ en ce sens que la plupart des débats peuvent être inscrits en opposition à ce courant⁴⁰.

1 – La conversation scientifique et l'organisation des théories des Relations Internationales.

La situation des Relations Internationales en fait un champ plural doté d'un socle ouvert à de nombreuses théories. Dario Battistella⁴¹ résume la situation ainsi : deux grandes conceptions scientifiques, trois traditions philosophiques et quatre débats inter-paradigmatiques. Les deux grandes conceptions scientifiques concurrentes pour étudier les Relations Internationales s'opposent dans leur rapport à la connaissance. La première conception entretient un rapport objectif à la connaissance, elle est dite « explicative ». Elle décrit les relations internationales comme le produit de causes objectives indépendantes de la connaissance des acteurs. Dans ce schéma, les causes ont toujours les mêmes effets. La seconde conception se situe dans un rapport de subjectivité de la connaissance, elle est dite « compréhensive ». Dans le cadre de cette conception, ce sont les acteurs et les contextes qui construisent le sens et le rôle de l'observateur est alors non plus d'expliquer mais d'interpréter les relations internationales à partir de ce point.

Les traditions philosophiques font référence à la fois à l'héritage philosophique préscientifique revendiqué de l'histoire des idées politiques ainsi qu'au postulat relatif à un état de nature particulier : soit l'absence *in abstracto* d'une autorité centrale supérieure à

³⁹ Sur le mésusage du mot paradigme pour qualifier des modes d'interprétations, voir notamment JACKSON Patrick Thaddeus et NEXON Daniel H., « Paradigmatic Faults in International-Relations Theory », *International Studies Quarterly*, vol. n° 53, n° 4, 2009, pp. 907 - 940. Voir aussi : MARTRES Jean-Louis, « De la nécessité d'une théorie des relations internationales : l'illusion paradigmique », *Annuaire Français de Relations Internationales*, vol. IV, 2003, pp. 22-28.

⁴⁰ Certains auteurs considèrent les grands débats inter-paradigmatiques comme une « déconstruction » progressive de la théorie réaliste où chaque théorie vient critiquer la théorie réaliste sur l'État, la puissance, l'intérêt, le rapport interne/externe ou encore les relations inter-étatiques. Voir notamment, MARTRES Jean-Louis, « De la nécessité d'une théorie des relations internationales : l'illusion paradigmique », *AFRI*, Vol. IV, 2003, pp. 19 - 41.

⁴¹ BATTISTELLA, *Théories des Relations Internationales*, op-cit., 2012 p. 123

l'acteur régalien détenteur de la souveraineté et qui définit les postulats des études traditionnelles : l'anarchie⁴² et la souveraineté⁴³. Lesquels constituent des inspirations des théories qui les ont suivies. Dans sa version « réaliste », l'anarchie se présente comme une structure déterminant les comportements des acteurs régaliens, acteurs de références⁴⁴. Dans sa version « libérale », l'anarchie n'est plus une structure déterminante mais une variable déterminée dans la rencontre des préférences subjectives de groupe d'individus, unités fondamentales de la scène internationale. Finalement dans sa version « globaliste », l'anarchie n'est qu'une étape dialectique dans l'émergence d'une communauté mondiale où l'humanité joue le rôle d'unité de base.

Dans leur manuel de 2001⁴⁵, plusieurs chercheurs Scott Burchill, Richard Devetak, Andrew Linklater, Matthew Paterson, Christian Reus-Smit et Jacqui True identifient neuf grandes familles de théories : Libéralisme, Réalisme (et néo-réalisme), Rationalisme, Marxisme, Théorie critique, Postmodernisme, Constructivisme, Féminisme et l'écologie (« *Green Politics* »). Dans leur version de 2013⁴⁶, les mêmes auteurs avec le renfort de Jack Donnelly et Terry Nardin, identifient également l'apport de la sociologie historique. La pensée de Marx s'ajoute aux approches marxistes, le rationalisme est abordé en tant que l'Ecole anglaise. Le chapitre sur le postmodernisme est devenu celui sur le poststructuralisme. Et les auteurs sont loin de parvenir à l'exhaustivité. Leur objectif est plutôt la restitution d'une vision contemporaine des questions posées par ces théories. Scott Burchill y développe une vision restreinte des théories qui se concentre sur ce qu'elle cherche à démontrer ou expliciter. Il y aurait tout d'abord des théories qui cherchent à expliquer les grandes lois de la politique internationale et/ou dégager les motifs récurrents d'appartenance nationale⁴⁷. Il ensuite

⁴² En réaction à une précédente typologie de Wight, Ibid. chapitres 1 et 2, pp. 13 – 79.

⁴³ Traduisant l'apport fondamental des sciences juridiques aux Relations Internationales dans la constitution du référentiel régalien.

⁴⁴ Dans un référentiel historique particulier, l'État n'ayant pas toujours existé, l'acteur régalien ne se comprend pas forcément comme tel.

⁴⁵ BURCHILL Scott, DEVETAK Richard, LINKLATER Andrew, PATERSON Matthew, REUS-SMIT Christian, TRUE Jacqui, *Theories of International Relations*, New York, Palgrave, 2^{ème} édition, 2001, 322 p.

⁴⁶ BURCHILL Scott, LINKLATER Andrew, DEVETAK Richard, DONNELLY Jack, NARDIN Terry, PATERSON Matthew, REUS-SMIT Christian, TRUE Jacqui, *Theories of International Relations*, New York, Palgrave, 5^{ème} édition, 2013, 396 p.

⁴⁷ Ibid p. 12. Scott Burchill fait référence aux travaux de Kenneth Waltz de 1979. WALTZ Kenneth, *Theory of International Politics*, McGraw-Hill, janvier 1979, 251 p.

identifie des théories issues de l'histoire et de la sociologie historique qui mettent en avant le principe de précaution face au caractère répétitif de l'histoire et la nécessité d'une analyse fondée sur le long-terme et les processus de développement pour dépasser l'évasive nature contemporaine des objets analysés⁴⁸. Les théories fondées sur les données empiriques⁴⁹, les théories comportementales basées sur l'explication et la prédiction des agissements des acteurs⁵⁰, les théories qui cherchent à préciser des usages de concepts⁵¹, forment un second ensemble d'objectifs auxquels les chercheurs ont pu souscrire. Le dernier ensemble est formé par les théories spéculatives sur les relations entre États et la nature de la société internationale (voir les conditions d'émergence d'une société monde)⁵², les théories critiques de la domination, ou de la justice ainsi que les théories cherchant à décrypter le processus de théorisation lui-même.

Dans une perspective inversée par rapport à l'historiographie classique et finalement de la construction de l'ouvrage, cette typologie interroge la nature et le contenu des théories des Relations Internationales. En effet, plusieurs auteurs (par exemple Martin Wight ou Andrew Linklater) se retrouvent ici dans plusieurs catégories de théories différentes. Les différences fondamentales entre certaines théories n'apparaissent pas clairement (théorie qui vise à définir les lois du système international/théories sur la nature de la société internationale). Et les écoles de pensées sélectionnées pour l'ouvrage ne se retrouvent que partiellement dans la typologie. Cela interroge également la place de l'auteur face à la

⁴⁸ Ibid. Dans cette catégorie, sont cités en exemple des travaux de plusieurs perspectives critiques différentes qui ont en commun des approches de long terme. Les auteurs mentionnés sont Linklater, Teschke ou encore les travaux de Rosenberg sur la technique : voir LINKLATER Andrew, *The Problem of Harm in World Politics: Theoretical Investigations*, Cambridge University Press, 2011. TESCHKE Benno, *The Myth of 1648: Class, Geopolitics and the Making of Modern International Relations*, Londres, Venno, 2003, - 308 p. ; ROSENBERG Nathan, *Exploring the Black Box: Technology, Economics, and History*, Cambridge University Press, 1994, 274 p.

⁴⁹ Par référence à l'emploi des données empiriques dans les travaux sur la paix perpétuelle de Michael W. Doyle de 1983 sur l'absence de conflit entre les démocraties-libérales. DOYLE Michael W. « Kant, Liberal Legacies, and Foreign Affairs », *Philosophy and Public Affairs*, Vol. 12, No. 3, Eté, 1983, pp. 205-235.

⁵⁰ Scott Burchill fait référence à l'ouvrage : HOLLIS Martin et SMITH Steve, *Explaining and Understanding International Relations*, Clarendon Press, 1990 226 p.

⁵¹ En plus de la mention des travaux classiques sur les causes de la guerre, l'auteur fait référence à la tentative de conciliation sur l'ordre et la justice de BUTTERFIELD Herbert et WIGHT Martin *Diplomatic investigations: Essays in the theory of international politics*, Crows Nest, Allen & Unwin, 1966, 227 p. ; ainsi que sur la causalité, KURKI Milja, *Causation in International Relations: Reclaiming Causal Analysis*, Caùbridge University Press, 2008, 309 p.

⁵² WIGHT Martin, *International Theory: The Three Traditions*, Holmes & Meier, 1991, 286 p.

dimension cognitive d'une théorie donnée et souligne la complexité qui peut exister à parler de Théories des Relations Internationales. Les auteurs ont une généralement une pensée riche et une vie académique qui l'est tout autant. Certains de ces auteurs sont issus de disciplines académiques différentes ou connaissent d'autres activités professionnelles (politiques, commerciales, littéraires...). A l'inverse, les théories et la littérature qui y sont consacrées viennent simplifier cette pensée jusqu'à la réduire à sa plus simple expression parfois caricaturale⁵³.

La typologie de Burchill *et al* leur permet d'envisager quatre grands enjeux qui ont structuré l'évolution des Relations Internationales contemporaines⁵⁴. Tout d'abord la question des acteurs dominants, autour de laquelle les auteurs soulignent un élargissement du concept d'acteurs de l'État régional vers les corporations transnationales, les classes sociales transnationales, les capitalistes de casino⁵⁵, les organisations internationales et non-gouvernementales, les mouvements sociaux et les organisations terroristes internationales. Vient ensuite la question des relations dominantes également inscrite dans une logique d'ouverture, passant des relations stratégiques entre grandes puissances, vers le commerce, la paix, et les relations de domination et dépendance entre un centre de l'économie mondialisée et ses périphéries. Sont également pris en compte les études sur le genre appliquées aux Relations Internationales, les rapports de solidarité internationale et la question des origines et des migrations de population. Les enjeux empiriques et éthiques forment les troisième et quatrième points d'évolution de la discipline. Ils sont également restitués dans une logique d'ouverture des enjeux classiques (les États et guerre) vers d'autres enjeux globaux (tournés vers l'économie et l'humain).

Ces différentes typologies présentes dans un même ouvrage mettent en lumière que la différence fondamentale entre deux théories des Relations Internationales (et leur caractère irréconciliable) procède davantage d'une différence de postulats perçus entre les auteurs que

⁵³ Un exemple usité de cette dégradation consiste en la fausse représentation des auteurs idéalistes et réalistes, les uns doux rêveurs gentils et pacifistes, les autres comme des cyniques calculateurs et belliqueux.

⁵⁴ Les auteurs rappellent la nature politisée qui discrimine souvent les bonnes théories des mauvaises. BURCHILL *et al*, Op-cit. p 14.

⁵⁵ Expression tirée de l'école de pensée de l'économie politique internationale et plus précisément des travaux de Susan Strange qui désigne la place trop grande accordée à la liberté et la valorisation dans domaine des marchés financiers par l'acteur étatique plutôt qu'à la sécurité et à la distribution des richesses.

de tout autre paramètre (phénomènes de continuité historique, objet d'analyse, méthode, but social...). La conceptualisation des théories relève ainsi de la capacité des théoriciens à synthétiser les postulats partagés par certains auteurs afin de justifier l'agrégation d'un auteur à un courant donné⁵⁶. Ainsi les Théories des Relations Internationales ne sont pas tant structurées par théories elles-mêmes et leur contenu qu'elles invitent à connaître mais plutôt des courants de pensée organisés pour rendre compte de l'évolution d'une discipline voir l'instituer comme telle parfois en discriminant les théories entre elles⁵⁷.

2 – Les grands débats, la classification des théories générales et débats sectoriels.

A l'image des théories, la première question à se poser lorsqu'on évoque ces débats, c'est celle de leur nombre ainsi que le nombre de théories qu'ils recouvrent. Qu'est-ce qui détermine qu'une vision du monde peut constituer une théorie et est suffisamment importante pour figurer parmi les grands débats ? Quelle classification opérer ? Là encore les avis divergent... Une constante parmi toutes ces classifications : les débats inter-paradigmatiques sont toujours associés à une décennie particulière. Par exemple, une classification de Katzenstein, Keohane et Kraser en 1999 que nous n'avons pas retenue⁵⁸, considère trois grandes questions autour de la construction des Relations Internationales : le débat entre idéalisme et réalisme dans les années 30, la discussion entre « néolibéraux » et « néoréalistes » dans les années 80 et enfin l'opposition « rationalisme » et « constructivisme » depuis les

⁵⁶ Pour un travail de cartographie des principaux courants voir : FRASSON-QUENOZ Florent, « An inclusive map of international relations theories and authors », *Cahiers du CIPE (Cuardernos del Centro de Investigaciones y Proyectos Especiales)*, Université Externado de Colombie, n°21, juin 2014, p. 21.

⁵⁷ Avec une efficacité très relative, étant donné qu'une théorie des Relations Internationales est invalidée que pour un motif extrinsèque. Elle n'est remise en cause que, si et seulement si, ses postulats majeurs tombent et non pas parce qu'elle ne marche pas.

⁵⁸ KATZENSTEIN Peter J. , KEOHANE Robert O. et KRASNER Stephen D. , « International Organization and the Study of World Politics », In. KATZENSTEIN Peter J. , KEOHANE Robert O. et KRASNER Stephen D. (dir.), *Exploration and Contestation in the Study of World Politics*, Massachusetts, MIT Press, 1999, pp. 12 - 30.

années 90. Dans le cadre de cette recherche, le point de départ était le modèle en quatre débats non-exclusifs décrit par Dario Battistella⁵⁹ ⁶⁰.

Le premier « grand débat » revêt une dimension téléologique : quel est le but de l'étude des Relations Internationales ? Ce premier échange opposerait dans l'entre-deux-guerres et l'après Seconde Guerre mondiale, des auteurs issus des courants « libéraux », parfois désignés comme « idéalistes »⁶¹, et les courants « réalistes »⁶². Les premiers penseraient que les Relations Internationales devraient être utilisées pour changer la politique internationale, tandis que les seconds prétendraient décrire les Relations Internationales telles qu'elles sont⁶³. En dehors du débat téléologique opposants réalistes et libéraux, il existe deux visions anthropologiques différentes qui s'opposent de façon un peu caricaturale : les réalistes considèrent que l'être humain est mauvais par nature, à l'inverse des libéraux. Cette considération se combine au postulat que la nature humaine emporte celle de l'État. Toutefois, ce débat procède essentiellement d'une reconstruction *a posteriori* dans un souci de légitimation du champ des Relations Internationales face à la Science Politique, au Droit et à

⁵⁹ Voir notamment le troisième chapitre de l'ouvrage BATTISTELLA Dario (2003), *Théories des Relations Internationales*, 4^{ème} éd., Paris, Presses de Science Po, 2012, pp 81 – 120.

⁶⁰ Il existe bien d'autres classifications se fondant sur un nombre de questions différentes. S'il en existe trois chez Katzenstein, Keohane et Krasner, il est possible de trouver des classifications à partir de nombres questions plus importants. Par exemple, la classification de Fred Chemoff identifie huit questions fondamentales. CHEMOFF Fred, *Theory and MÉtatheory in International Relations : Concepts and Contending Accounts*, New York, Palgrave Macmillan, 2007, pp. 40-46.

⁶¹ Les auteurs décrits comme libéraux sont Norman Angell, G. Lowes Dickinson, John Hobson, Leonard Woolf ou encore Alfred Zimmern. Le courant libéral a évolué durant la guerre froide avec les travaux sur l'intégration et les régimes politiques, avant de subsister dans l'école anglaise.

⁶² Du côté réaliste les auteurs associés ou s'y inscrivant plus ou moins directement malgré leurs nombreuses différences sont Reinhold Niebuhr, Edward Hallett Carr précurseurs du courants, Hans Morgenthau, Raymond Aron et Henry Kissinger. Le courant réaliste perdura sous de nouvelles formes avec de nouveaux auteurs suivants qui s'inscriront dans diverses approches « néoréalistes » et notamment Kenneth Waltz, Robert Gilpin, Joseph Grieco, Robert Jervis, John Mearsheimer, Jack Snyder, Stephen Walt [...].

⁶³ Le débat relève davantage d'une forme de succession dans le temps.

l’Histoire⁶⁴. Le « débat » entre réalistes et libéraux a eu lieu après la Seconde Guerre mondiale et opposait plutôt les chercheurs sur la question d’un intérêt national américain⁶⁵.

Il est important ici d’ouvrir une parenthèse sur les approches libérale et réaliste en ce qu’elles déterminent les oppositions à venir. Dans une optique réaliste, l’État est la principale unité d’analyse d’un système international. Il agit de manière rationnelle à partir des informations qu’il possède pour satisfaire ses intérêts. Il en résulte que le pouvoir et la sécurité sont les valeurs fondamentales de cet agent. En tant qu’entité politique souveraine, l’État vit dans un système international caractérisé par l’absence de gouvernement central qui oblige les États à agir en dehors de leurs espaces nationaux. Cette situation qualifiée plus tard d’anarchie conduit fatalement les États à se poser la question du dilemme de sécurité. L’accroissement de la puissance militaire d’un État, perçu comme une menace par les autres États, amène ceux-ci à accroître leur propre puissance militaire⁶⁶. A l’inverse, le courant libéral est un courant théorique beaucoup plus large et diversifié qui ira de l’approche dite « idéaliste » de Wilson jusqu’au théories néolibérales, en incluant les théories de la paix démocratique, de l’interdépendance, de la seconde-image ainsi que les approches domestiques et bureaucratiques de la politique internationale. L’ensemble de ces théories se distinguent des hypothèses réalistes en ce qu’elles insistent sur la pluralité des acteurs, les relations entre les dimensions internes et externes de la politique des États, l’existence de normes et d’institutions internationales, et sur le fait que la survie ne constitue pas le seul intérêt de l’État. Là où ces deux approches paradigmatisques se rejoignent c’est sur le fond épistémologique et méthodologique. Elles mettent toutes les deux l’accent sur l’interaction basée sur différents intérêts tout en ayant recours à des méthodes similaires incluant le recours à des principes philosophiques inscrit sur un fond historique.

⁶⁴ SCHMIDT Brian C. , *International Relations and the First Great Debate*, Londres, Routledge, 2012, 192 p. Pour une histoire récente des prémisses de la discipline voir également du même auteur : SCHMIDT Brian C. (1998) *Political Discourse of Anarchy, The: A Disciplinary History of International Relations*, New York, SUNY Press, 2016, 309 p.

⁶⁵ Pour une restitution qui s’affranchit des caricatures entre libéraux pacifistes et réalistes cyniques, voir l’ouvrage déjà cité en ses chapitres 6 et 7, SCHMIDT Brian C. , *International Relations and the First Great Debate*, op-cit. pp. 94 – 132.

⁶⁶ HERZ, John H. *Political Realism and Political Idealism: a Study in Theories and Realities*. University of Chicago Press, 1951, 275 p.

La méthodologie des Relations Internationales fait l'objet d'un deuxième débat entre les approches bémorioristes et les approches dites traditionnalistes⁶⁷. Ce débat qui existe entre les années 50 et 70 est souvent résumé à une querelle d'une approche tirée de la philosophie et de l'histoire contre une approche formelle ou/et quantitative qui recherche les lois du comportement (*behavior*) des acteurs⁶⁸. Le bémoriorisme est introduit au sein des Relations Internationales à travers des approches décisionnelles⁶⁹ et formera notamment un socle pour les approches systémiques ainsi que de nouveaux sous-champ des Relations Internationales tels l'analyse de la politique étrangère. Ce débat n'a pas de vainqueur dans la mesure où si l'apport de l'empirie est reconnu, celle-ci ne peut faire l'économie des approches théoriques. Les auteurs s'opposent sur le statut de ce second débat. Pour certains auteurs, il est un simple débat méthodologique qui ne remet pas en cause les approches traditionnalistes, voire peut s'envisager de simple manière complémentaire⁷⁰. Pour d'autres, il s'agit d'une révolution⁷¹. Sur les aspects quantitatif, la méthodologie actuelle des Relations Internationales a évolué à la marge de celles-ci depuis le milieu des années 90⁷². Bien que le présent objet d'étude, avec d'autres, participent du renouvellement de ce débat méthodologique⁷³.

⁶⁷ Le débat ne consiste pas en une opposition frontale. D'une part, il est synonyme d'une ouverture de la discipline à d'autres approches issues des mathématiques, de l'économie, de la biologie... D'autre part, certains bémorioristes apportent l'empirie aux théories réalistes ou demeurent assez proches des postulats des réalistes (Morton Kaplan, David Singer, Melvin Small, Thomas Schelling, James Rosenau), d'autres proposent de nouvelles approches, notamment les (précurseurs) transnationalistes tels John Burton ou encore l'approche cybernétique des travaux de Karl Deutsch sur laquelle nous reviendrons.

⁶⁸ L'approche formelle se comprend ici comme la logique et les mathématiques, tandis que l'approche quantitative se comprend comme la démarche empirique des sciences sociales et des sciences naturelles.

⁶⁹ Notamment les travaux SNYDER Richard C., BRUCK Henry W. et SAPIN Burton M. (dir), (1954), *Foreign Policy Decision Making: An Approach to the Study of International Politics*, Literary Licensing, LLC, 2012, 286 p.

⁷⁰ Notamment du fait de son caractère incomplet, focalisé avant tout sur les méthodes positivistes opposée à l'histoire plutôt que sur les mérites de l'enquête sociale. CURTIS Simon., & KOIVISTO, Marjo. « Towards a second "second debate"? Rethinking the relationship between science and history in international theory ». *International Relations*, 24, décembre 2010, pp. 433-455.

⁷¹ Plus ancienne, cette opinion est notamment défendue par LIJPHART Arend, « The Structure of the Theoretical Revolution in International Relations », *International Studies Quarterly*, Vol. 18, No. 1, Mars 1974, pp. 41-74.

⁷² KING Gary, KEOHANE Robert O. et SIDNEY Verba, *Designing Social Inquiry: Scientific Inference in Qualitative Research*, Princeton University Press, 1994,

⁷³ Cf. chapitre 6.

La troisième question des Relations Internationales concerne la nature régaliennes de l'acteur des Relations Internationales⁷⁴. Elle relève donc de l'ontologie. L'État est-il le seul acteur à considérer au sein des Relations Internationales ? Ce débat oppose ainsi des approches stato-centrées étudiant les relations de guerre et de paix entre ensembles régaliens⁷⁵, à des visions prônant l'étude des relations transnationales de toute nature entre tous acteurs, essentiellement portées par les approches critiques, transnationalistes et marxistes. Ce troisième débat est également le point de départ de l'intégration du constructivisme⁷⁶. D'un point de vue épistémologique, ce débat s'inscrit en rupture avec l'héritage philosophique⁷⁷ car il remet en cause la spécificité de l'acteur des relations internationales : la souveraineté, et donc l'anarchie. Plutôt que deux approches, ce débat va mettre en scène plusieurs « acteurs » ou référents analytiques : système ou société d'État, États, groupes d'individus, individus, structures sociales, humanité. Ainsi, les différents auteurs se rangeront moins par théories d'appartenance que par niveau d'analyse. Si on prend l'exemple de l'école anglaise, des auteurs plus proches des postulats réalistes à l'image de Martin Wight ou Hedley Bull seront concernés par les États et les sociétés d'États tandis que des auteurs avec une approche plus libérale comme Raymond Vincent ou constructiviste comme Nicholas Wheeler seront davantage placés vers les groupes d'individus et les individus (encore une fois ce sont les postulats qui détermineraient cette partition). Bien que comme tout débat il emporte des considérations épistémologiques, l'épistémologie forme davantage le cœur du quatrième débat. La connaissance scientifique des relations internationales est-elle possible ? Il oppose des approches positivistes qui l'affirment, aux approches post-positivistes ou réflexives⁷⁸ qui

⁷⁴ Ce troisième débat semble être le plus actif. Il intégrerait ainsi deux types d'enjeux contemporains relevés par Burchill *et al.*, précité, non seulement les acteurs mais également la question des relations entre ceux-ci

⁷⁵ États et autres entités et accords issus de la volonté régaliennes.

⁷⁶ Ensemble varié de courants dans avec notamment : Les travaux d'Alexander Wendt et tout particulièrement WENDT Alexander, « Anarchy Is What States Make of It. The Social Construction of Power Politics » (1992), in DER DERIAN James (dir.), *International Theory. Critical Investigations*, Basingstoke, Palgrave Macmillan, 1995, pp. 129 -177. Sur les structures et le rôle des normes et du langage, voir notamment les travaux de Nicholas Onuf : ONUF Nicholas G., *World of Our Making: Rules and Rule in Social Theory and International Relations*, Routledge, 2012, 340 p. exemple les travaux de Margaret Keck, Kathryn Sikkink sur la société civile et les droits de l'homme. Voir : KECK Margaret E, et SIKKINK Katheryn, *Activists beyond Borders: Advocacy Networks in International Politics*, Ithaca, Cornell University Press, 1999, 240 p On peut également penser aux travaux de Maja Zehfuss : ZEHFUSS, Maja « Contemporary western war and the idea of humanity » In *Environment & Planning D: Society & Space*. 30, 5, 2012, pp. 861-876.

⁷⁷ Cf. supra.

⁷⁸ Les approches décrites comme « post-positivistes » laissent place à des travaux réflexifs sur les Relations Internationales parmi lesquels se trouvent ceux de Robert Cox, d'Andrew Linklater, de Richard Devetak, de James Der Derian ou encore de Richard K. Ashley...

en doutent. Ce débat est réputé être celui des années 80/90, mais il se poursuivrait toujours. De manière générale, les approches post-positivistes sont hétérogènes et mettent en avant plusieurs épistémologies différentes (théorie critique, féminisme, post-modernisme...) qu'il convient de distinguer.

Hors l'avantage pédagogique qui consiste en la simplification de la connaissance autour de nombreux auteurs et de leurs écrits dans un ensemble de théories non-figées, l'avantage principal du modèle des grands débats réside dans les questions qu'il pose. Ce modèle permet d'interroger fondamentalement la recherche en Relations Internationales en termes d'objectifs, de méthode, d'objets et de faisabilité. Toutefois, cette utilité ne vaut que sous la triple réserve suivante : premièrement, les débats doivent être ouverts à de nouvelles théories et ne pas être considérés comme historiquement clos. Deuxièmement, un débat n'en remplace pas un autre. Troisièmement, les débats doivent être envisagés de manière non-exclusive. Autrement dit, chaque débat possède une dimension formelle et un contenu, ainsi qu'une dimension épistémologique et ontologique.

Ces précautions sont nécessaires pour pouvoir contrevenir aux nombreuses limites du modèle des grands débats. Le modèle des grands débats entretient un rapport distant à la vérité que celle-ci soit considérée comme le reflet d'une réalité objective, un élément de cohérence pratique ou une vision consensuelle. Ceux-ci sont souvent « faux »⁷⁹, incomplets⁸⁰, insolubles et déliés des objets d'analyses des théories qu'ils invoquent, (théories à vocation les plus générales possibles). Finalement, l'avantage du modèle se perdrait et cantonnerait le chercheur à l'option pour certaines théories et à la promotion militante de celles-ci. Cela est d'autant plus vrai que le phénomène théorique des Relations Internationales dépasse de loin les théories générales. La majeure partie de la production académique du champ n'étant pas consacrée à celles-ci mais à des débats sectoriels qui forment autant de processus et de domaines d'étude particuliers. Le *Traité de Relations Internationales* de Frédéric Ramel et Thierry Balzacq⁸¹ référence 16 de ces domaines⁸² ou axes de recherche. Il s'agit de l'une des

⁷⁹ Dans leur effectivité, leur bornage chronologique ou dans le lien affilant un auteur à un courant donné.

⁸⁰ Il y aura des théories qui manquent et les débats seront insuffisants pour restituer la richesse et l'évolution des travaux d'un auteur ou l'ensemble des débats périphériques qui peuvent être conduits dans la discipline.

⁸¹ BALZACQ Thierry et RAMEL Frédéric (dir.), *Traité de Relations Internationales*, Paris, Presses de Science Po, 2013. 1232 p.

⁸² Ibid, partie 3, pp. 525 - 1054.

présentations les plus complètes : L'analyse et la résolution des conflits, la diplomatie publique, le droit international, l'économie politique internationale, l'éthique, les études de sécurité, la stratégie, la géopolitique, l'histoire, la négociation internationale, les organisations internationales, la philosophie, la politique étrangère, la psychologie politique internationale, les Théories des Relations Internationales, l'environnement⁸³. L'ensemble théorique formé est vaste et il s'accroît d'année en année et nourrit une production métathéorique⁸⁴.

Ainsi la première précaution face à cet « éclatement » de la théorie consiste à se méfier tout particulièrement du vocabulaire qui encadre ce foisonnement théorique tant il diverge parfois de la Science Politique⁸⁵ : parmi d'autres exemples, le réalisme des Relations Internationales n'est pas le réalisme philosophique ou encore le constructivisme d'Alexander Wendt n'est pas le constructivisme des autres sciences sociales. Il en va de même pour les postulats antagonistes idéologiquement marqués.

3 – Rejet, monisme et pluralisme : des approches *theory-driven* aux approches *problem-driven*.

Plusieurs attitudes existent face à ces théories déterminées par le degré de pluralisme admis par le chercheur⁸⁶. La première attitude consiste tout simplement à rejeter la source de connaissance que constituent les Théories des Relations Internationales par la controverse ou le passage sous silence. L'argument de ces approches est souvent caricatural et repose sur la double idée qu'il y a trop de théories et qu'elles ne regardent que la théorie dans une compréhension « métaphysique » du monde⁸⁷. Un tel raisonnement méconnait l'aspect construit de ces mêmes théories qui en dehors de leurs dénominations et regroupements

⁸³ Evidemment, chacun de ces domaines peut être compris de façon matricielle de nombreux univers disciplinaires qui ne relèvent pas tous de la Science Politique dans l'ensemble de ses décompositions (Philosophie et théorie politiques, sociologie politique, politiques publiques, sciences administratives ou relations internationales), mais peut se nourrir de travaux en économie, en histoire, en géographie, en psychologie, en mathématiques et bien sûr en droit. Ibid.

⁸⁴ Entendue au sens d'Habermas, une théorie ayant pour objet une théorie, voir HABERMAS Jürgen (1968), *La Technique et la science comme « idéologie »*, Paris, Gallimard, 1990, 211 p.

⁸⁵ Certains auteurs suggèrent d'ailleurs d'écartez la « littérature » des Relations Internationales sauf à employer les termes entre guillemets car d'un usage erroné : DOGAN Mattei, « The Hybridization of Social Science Knowledge », *Library Trends*, vol. 45, n° 2, 1996, pp. 299-301.

⁸⁶ Bien que les conflits entre paradigmes relèvent d'une dimension construite par celui-ci, et que les oppositions dans la production scientifique ne soit pas si marquée que dans l'enseignement des Relations Internationales.

⁸⁷ Cf. supra.

parfois discutables, possèdent un contenu riche qui n'exclut pas le réel dans la mesure où il s'inscrit la plupart du temps dans un objectif de légitimation ou de contestation du pouvoir. Par ailleurs, cette posture est loin d'exclure la traductibilité de ces mêmes approches sous l'angle des théories⁸⁸. Une seconde tendance se trouveraient dans les approches dites « monistes » dont le fondement repose sur la sélection d'une théorie ou d'un courant donné. Ces approches monistes se déclinerait ensuite selon le degré de militantisme de l'auteur : d'une explication monolithique des phénomènes politiques internationaux à la lutte pour l'imposition d'un modèle de pensé face aux autres modèles. Autrement dit, le monisme de déclinerait de la simple proposition concourante vers une compétition paradigmique⁸⁹. Enfin, le « pluralisme » consiste à admettre à divers degrés la pluralité des théories et à considérer cette pluralité ne constitue non pas une faiblesse des Relations Internationales. Plusieurs exemples de « pluralisme » existent dans les Relations Internationales. Le premier rapprochement se situe dans la synthèse « neo-neo »⁹⁰ dite « rationaliste » par Keohane⁹¹. Cette synthèse entre néoréalisme et néolibéralisme manifeste l'expression d'un positivisme en Relations Internationales contre laquelle les alternatives post-positivistes, critiques ou radicales s'affirment et se structurent⁹². Un autre exemple de pluralisme réside dans la nouvelle approche dominante libéralo-constructiviste. Celle-ci se retrouve notamment dans les travaux conjoints de Keohane, Krasner et Katzenstein pour une complémentarité des approches rationalistes (plutôt dans son versant libéral) et constructivistes⁹³. Cette complémentarité est affirmée également par Fearon et Wendt qui pensent qu'il faut aborder le constructivisme davantage comme un outil que comme une compréhension métaphysique

⁸⁸ BATTISTELLA, op-cit. p. 712.

⁸⁹ C'est ce que Gunther Hellmann désigne comme une forme particulière de monisme, le « paradigmisme » soit la compétition pour accéder au statut de paradigme et le devoir d'adopter strictement un camp. Voir notamment HELLMANN Gunther « Brother, Can You Spare a Paradigm? (Or Was Anybody Ever a Realist?) », *International security*, 25(1), 2000 pp. 169 – 174 ainsi que HELLMANN Gunther (dir.), « The Forum : Are Dialogue and Synthesis Possible in International Relations ? », *International Studies Review*, vol. II, 2003.

⁹⁰ Pour reprendre l'expression d'Ole Wæver. WÆVER Ole., « The rise and fall of the inter-paradigm debate », in SMITH Steve, BOOTH Ken., ZALEWSKI Marysia (eds.), *International Theory: Positivism and Beyond*, Cambridge, Cambridge University Press, 1996, pp. 149-185.

⁹¹ KEOHANE Robert, « International institutions : two approaches », *International Studies Quarterly*, vol. 32, n°4, 1988, pp. 379-396.

⁹² Sur le caractère « hégémonique » et résistance américaine de cette synthèse face aux approches alternatives voir MACLEOD Alex « Emergence d'un paradigme hégémonique » In. MACLEOD Alex et O'MEARA Dan (dir.), *Théories des relations internationales. Contestations et résistances*, Montréal, Athéna éditions, 2007, pp. 19-34.

⁹³ KATZENSTEIN Peter J. , KEOHANE Robert O. et KRASNER Stephen D., op-cit.

du monde et qu'il s'inscrivait moins dans un « débat » avec le rationalisme que dans une « conversation »⁹⁴ ⁹⁵. Bien que cette synthèse ignore une partie du rationalisme notamment la partie issue du néoréalisme. Au-delà de ces exemples, le pluralisme prend également la forme du dépassement des débats antérieurs et privilégier une vision pragmatique et éclectique des phénomènes internationaux qui ne sont plus guidées par la théorie ou « *theory-driven* » mais fondée sur l'apport de connaissances applicables à l'étude des problématiques soulevées par ces phénomènes. La recherche est donc décrite comme guidée par celles-ci ou « *problem-driven* ».

B – Approches éclectiques et objets complexes : le pragmatisme « *problem-driven* ».

Les approches dites *problem-driven* soulèvent la question de la « combinaison » des objets issus de plusieurs sources théoriques⁹⁶. Cette question de la combinaison a fait l'objet des travaux de thèse de Jérémie Cornut desquels cette présente recherche d'inspire⁹⁷. Dans son introduction, l'auteur énumère les différents types d'approches pluralistes : comptabiliste, dialogique et combinatoire⁹⁸. Jérémie Cornut décrit une combinaison fondée sur la

⁹⁴ FEARON James D. et WENDT Alexander, « Rationalism vs constructivism. A Skeptical view » In. CARLSNAES Walter, RISSE Thomas et SIMMONS Beth, *Handbook of international relations*, sage, 2002, pp 52 – 72.

⁹⁵ On peut également faire référence à l'approche du rationalisme d'Andrew Moravcsick pour qui ce dernier comprend les théories de la distribution internationale des ressources (réalisme), des préférences (libéralisme), de l'information (institutionnalisme) et des croyances (constructivisme). MORAVCSICK Andrew « Liberal International Relations Theory : A Scientific Assessment » in ELMAN Colin et FENDIUS ELMAN Miriam (eds) *Progress in International Relations Theory: Appraising the Field*, Cambridge, MIT Press, 2003, pp. 159-204

⁹⁶ La combinaison peut également être rapprochée de l'assemblage. Sur la notion d'assemblage, voir ACUTO Michele et CURTIS Simon (eds), *Reassembling International Theory. Assemblage Thinking and International Relations*, Londres, Palgrave, 2013, 158 p.

⁹⁷ CORNUT Jérémie, *Le pragmatisme et l'analyse des phénomènes complexes dans la théorie des relations internationales : le cas des excuses dans la diplomatie américaine*, thèse de Science Politique, dirigée par BATTISTELLA Dario et ROUSSEL Stéphane, soutenue en 2012, 329 p. Nous avons travaillé avec la version disponible sur le site de l'Université du Québec à Montréal : www.archipel.uqam.ca/5014/1/D2325.pdf (lien toujours fonctionnel le 12 janvier 2017. Néanmoins cette thèse à fait l'objet d'une publication : *Les excuses dans la diplomatie américaine : Pour une approche pluraliste des relations internationales*, Montréal Les Presses de l'Université de Montréal, 2014, 189 p.

⁹⁸ Il se fonde ici sur la typologie du pluralisme de Richard Bernstein. La vision « comptabiliste » se limite à une approche mais reconnaît l'existence et la valeur d'autres. La vision « dialogique » sépare les différentes approches mais souhaite construire un échange entre elles. Les approches « combinatoires » pense que plusieurs théories peuvent expliquer un phénomène et que son étude exige la réunion de ces théories à vocation spécifique (pragmatisme centré sur l'objet) ou à vocation générale (synthèse théorique centrée sur une nouvelle théorie). BERNSTEIN Richard, « Pragmatism, Pluralism and the Healing of Wounds », *Proceedings and Addresses of the American Philosophical Association*, Vol. 63, No. 3, Nov., 1989, pp. 5-18

philosophie pragmatique, qu'il désigne sous l'appellation « pragmatisme *problem-driven* ». L'idée est de combiner les théories afin de cerner les phénomènes politiques internationaux en « refusant » le paradigmatisme⁹⁹. Cette combinaison est rendue possible au travers d'une recherche conduite par des problèmes spécifiques et envisageant les théories comme des outils complémentaires destinés à une compréhension holistique du phénomène. Cette approche est notamment construite sur la base des travaux sur le réalisme pragmatique d'Hilary Putnam¹⁰⁰ ainsi que des travaux communs et respectifs de Sil et Katzenstein concernant l'éclectisme analytique¹⁰¹.

Le « pragmatisme conduit par les problèmes » et l'éclectique analytique entretiennent un rapport complexe. L'éclectisme analytique est introduit dans le champ des Relations Internationales par les travaux de Rudra Sil entre 2000 et 2004, puis avec Peter Katzenstein à partir de 2005¹⁰² jusqu'en 2010¹⁰³. Les deux approches ont des objectifs identiques et peuvent être classés dans les approches pragmatiques. Par ailleurs, les deux approches ont des éléments épistémologiques commun. La différence essentielle entre les deux approches procède des dimensions téléologique et épistémologique. D'une part, en ayant recours au réalisme de Putnam, Jérémie Cornut renforce la dimension épistémologique en construisant des outils conceptuels qui viennent préciser cette première théorie. D'autre part, le pragmatisme conduit par les problèmes n'a pas vocation à les résoudre mais à les comprendre. Le pragmatisme « *problem-driven* » n'est pas « *problem-solving* » à la différence de l'optique utilitariste souhaitée par Sil et Katzenstein. Une autre différence réside dans l'ouverture limitée de

⁹⁹ Avec une nuance dans le fait que « Sans une analyse paradigmatische le pragmatisme est dépourvu des outils qui lui permettent de mener une étude éclectique ». CORNUT, op-cit. p. 277.

¹⁰⁰ A la fois pour le « réalisme interne » (« si la vérité est en partie un construit social, des éléments extérieurs permettent de distinguer le vrai du faux ») mais également pour ses travaux sur la diplomatie, et en opposition avec les travaux de Richard Rorty. CORNUT op-cit. pp. 77 - 124 puis pp. 207 - 241

¹⁰¹ De manière générale pour l'influence du pragmatisme sur les Relations Internationales voir l'ouvrage collectif BAUER, Harry et BRIGHI Elisabetta (dir.) *Pragmatism in International Relations*. New York, Routledge, 2009, 208 p.

¹⁰² KATZENSTEIN Peter J. et SIL Rudra « What is analytic eclecticism and why do we need it ? A pragmatist Perspective on Problems and Mechanisms in the Study of World Politics », intervention au colloque annuel de l'*American Political Science Association* le 1^{er} septembre 2005.

¹⁰³ Essentiellement les précisions apportées dans l'ouvrage : SIL Rudra et KATZENSTEIN Peter J., *Beyond Paradigms: Analytic Eclecticism in the Study of World Politics*, Macmillan, 2010, 240 p.

l'éclectisme analytique au libéralisme, au réalisme et au constructivisme parce que ce sont les approches les plus « répandues » aux États-Unis et dans le reste du monde^{104 105}.

En tant que telle, l'éclectisme analytique prête le flanc aux remises en cause qui lui trouvent une vocation à perpétuer la domination des courants américains dominants sur la discipline¹⁰⁶. Enfin, le pragmatisme de Jérémie Cornut admet la nature nécessairement incomplète de la compréhension des phénomènes étudiés. Le « pragmatisme conduit par les problèmes » s'oppose également en la matière à la démarche de la synthèse théorique qui a vocation à créer une théorie plus complète à partir des théories existantes. Il n'y a pas de vocation à imaginer une nouvelle école des Relations Internationales mais à être inclusif et construit autour d'une importante casuistique. Pour Jérémie Cornut, la synthèse théorique est moins conduite par les problèmes que par les théories¹⁰⁷. Par ailleurs, bien que pluraliste *ab initio* une synthèse opère un produit clos et confine finalement au paradigmatisme, tandis le pragmatisme est ouvert à de nouvelles compréhensions. Du point de vue de la Science Politique, la thèse de Jérémie Cornut à travers l'utilisation du réalisme interne Putnam s'inscrit dans une forme de « réalisme critique » qui se focalise davantage sur la recherche de contingences des phénomènes étudiés que sur leurs régularités. Ontologiquement, les théories en compétition se réfèrent à un monde extérieur commun¹⁰⁸. Téléologiquement, la recherche de l'ensemble des informations relatives à la compréhension d'un phénomène international est réaliste¹⁰⁹. La mise en avant du caractère réaliste de cette approche est l'occasion d'évoquer les trois outils mis en place : le texte explicatif idéal, l'érotétique et la sélection des théories.

¹⁰⁴ KATZENSTEIN et SIL, 2010, p. 36.

¹⁰⁵ Ce point conduit Jérémie Cornut à affirmer que les auteurs ne perçoivent pas fondamentalement de différence entre l'éclectisme et une théorie de moyenne portée. Op-cit. p. 269

¹⁰⁶ Voir notamment MACLEOD, 2007 op-cit.

¹⁰⁷ CORNUT, op-cit. p. 271.

¹⁰⁸ SMITH Steve, « Dialogue and the Reinforcement of Orthodoxy in International Relations », *International Studies Review*, Vol. 5, I1, Mars 2003, pp. 141–143,

¹⁰⁹ Cf. supra.

1 – Le pragmatisme conduit par les problèmes : à la recherche du texte explicatif idéal.

Parmi les obstacles au pragmatisme, Jérémie Cornut soulève l'idée de l'intégration de théories contradictoires au sein de la même analyse¹¹⁰. Sans nous attarder sur la dimension téléologique du conseil du Prince, nous nous focaliserons ici sur la dimension ontologique de la combinaison destinée à répondre à la critique de l'incohérence ainsi que la question de la sélection des théories (ou des critères d'inclusions et d'exclusions de celle-ci). Conceptualisé par Railton¹¹¹, le texte explicatif idéal est l'outil conceptuel qui guide cette méthode de recherche. Il représente une image la plus complète d'un phénomène étudié garantissant à chaque perspective une « représentation juste de ses dynamiques »¹¹². Il est constitué par tous les outils théoriques qui permettent l'explication d'un phénomène donné dans tous ses aspects. Le texte explicatif idéal est en ce sens la somme de toutes les explications possibles d'un phénomène étudié.

Il est dit « idéal » car on ne peut pas l'écrire. Il est inatteignable et ouvert à l'intégration de nouvelles théories voire de nouvelles disciplines¹¹³. Son objectif est d'aider la compréhension en parvenant à la meilleure possible¹¹⁴. Autrement dit, une recherche en tant que telle n'est jamais terminée. Cette nécessaire incomplétude pousse le chercheur à être ouvert à l'ensemble des théories et à sélectionner les meilleures d'entre elles pour expliquer le phénomène donné. Dans cette sélection et cet usage chacune des théories vient répondre à

¹¹⁰ Ces développements font l'objet de son chapitre 3, CORNUT, op-cit pp. 125 – 181.

¹¹¹ RAILTON, Peter, « Probability, explanation, and information ». *Synthese* 48, 1981, pp. 233 - 256. Jérémie Cornut fait également référence à la lecture de Railton par Førland sous l'angle de l'écuménisme théorique appliqué à l'histoire. FØRLAND Tor Egil, « The Ideal Explanatory Text in History: A Plea for Ecumenism », *History and Theory*, Volume 43, Issue 3, Oct. 2004, pp. 321–340

¹¹² HERMANN Margaret, « One Field, Many Perspectives: Building the Foundations for Dialogue: 1998 ISA Presidential Address », *International Studies Quarterly*, Volume 42, Issue 4, 1 Déc. 1998, pp. 605–624,

¹¹³ Cette idée d'ouverture bien que déjà présente chez Railton en 1981 est reprise chez les autres auteurs utilisant le concept dont Jérémie Cornut, Margaret Hermann, Tor Egil Førland déjà cités.

¹¹⁴ FØRLAND, 2004, op-cit.

une question précise qui est elle-même intégrée dans une question plus vaste : « Une théorie est une explication, et cette explication est la réponse à une question »¹¹⁵.

2 – Réunir des théories contradictoires : L'érotétique ou la logique des questions.

Afin de permettre la combinaison, l'auteur mobilise une branche de la philosophie des sciences et de la logique : l'érotétique ou la logique des questions. Celle-ci résulte dans les sciences sociales d'un apport de Garfinkel¹¹⁶. Puisque différentes théories constituent des réponses à différentes questions, leur variété n'est pas source d'incohérence. Plus encore la variété devient un avantage par la détermination des « espaces contrastifs » réciproques de chacune des théories mobilisées. Ces espaces contrastifs représentent la relativité explicative de chacune des théories liées à leur contexte (« théorie du contraste » opposée à la « théorie propositionnelle »¹¹⁷). Selon cette théorie, toute réponse à une question est relative au contexte dans lequel elle est posée, le rôle de la théorie du contraste est de préciser les présupposés qui encadrent la question et de circonscrire la réponse attendue et donc l'attente de la personne qui pose la question¹¹⁸. Appliqué aux théories, cet outil permet de construire des liens entre elles. Il permet de circonscrire ce qui est une bonne explication dans le contexte de la question, ce qui est expliqué (l'espace contrastif), et ce qui n'est pas expliqué (l'extérieur de l'espace contrastif) et donc de construire un cadre de travail pour estimer la pluralité des explications tout en évitant la menace de l'incohérence¹¹⁹. Avec l'application de cet outil aux Relations Internationales, Jérémie Cornut entend la compatibilité et la complémentarité des différentes théories parce qu'elles répondent à des questions complémentaires.

¹¹⁵ CORNUT, op-cit, p. 133. Lequel s'inscrit ici dans l'approche de Garfinkel qui suppose que même si la théorie ne se présente pas sous la forme d'une question, il faut quand même se demander à quelle question elle répond. GARFINKEL Alan, *Forms of Explanation: Rethinking the Questions in Social Theory*, Yale University Press, 1981 - 186 p.

¹¹⁶ GARFINKEL, 1981, op-cit.

¹¹⁷ La théorie qui veut que la réponse à une question soit indépendante de la structure de celle-ci CORNUT, op-cit. p 143. Pour une critique de la différence entre théorie prépositionnelle et théorie du contraste voir l'article : TEMPLE Dennis The Contrast Theory of Why-Questions », *Philosophy of Science*, 55, n° 1, mars 1988, pp. 141-151. Voir également sur l'intérêt et les limites du contraste : YLIKOSKI Petri «The Idea of Contrastive Explanandum». In PERSSON Johannes et YLIKOSKI Petri (dir.), *Rethinking Explanation*. Dordrecht: Springer, 2007 pp. 27-42

¹¹⁸ Jérémie Cornut reprend ici l'idée du « sachant que » ou « given clause » de Garfinkel. CORNUT, op-cit. p 142.

¹¹⁹ En ce sens : DE LANGHE Rogier, WEBER Erik, VAN BOUWE Jeroen, « A pragmatist approach to the plurality of explanations in International Relations Theory Graham Allison's account of the Cuban Missile Crisis reconsidered » 2007, 17 p.

« Lorsque deux questions sont complémentaires, les explications qui répondent à ces questions le sont aussi. Par extension, il en est de même pour les théories qui fournissent ces explications complémentaires. Or, en général, une question en cache plusieurs autres, pour deux raisons liées entre elles : elle présuppose souvent des éléments clarifiés par d'autres, parce que les phénomènes sociaux sont trop complexes pour pouvoir être étudiés avec une seule théorie »¹²⁰.

Il inscrit dans cette démarche les travaux d'Alexander Wendt¹²¹, mais également ceux de Thomas Lindemann¹²² ainsi que les travaux de Lisa Wedeen¹²³. L'auteur opère une analyse des travaux de Milja Kurki, dont il présente les observations critiques sur la nature de la cause retenue par les positivistes et les post-positivistes qui se focalise sur la cause « efficiente » (au sens d'efficace). Milja Kurki propose de revenir à la conception aristotélicienne de la causalité appliquée aux phénomènes politiques¹²⁴. Dans une volonté explicative multi-causale, cette conception revient à pouvoir ajouter à la cause positiviste, les idées, les règles, les normes et les discours¹²⁵.

3 – L'inclusion et l'exclusion des théories par la sélection pragmatique

La sélection d'une théorie en tant qu'explication est déterminée non par son degré de « vérité », mais son « degré de pertinence ». Ce degré de pertinence est défini par la négative de telle sorte qu'il peut être qualifié de degré de non-pertinence résiduel minimal. Une théorie sera pertinente en tant qu'explication quand elle ne sera ni « fausse », ni « objectivement non-

¹²⁰ CORNUT, op-cit. pp. 146 – 147.

¹²¹ WENDT Alexander, op-cit. ainsi que FEARON et WENDT, op-cit.,

¹²² En particulier les travaux combinant constructivisme et réalisme sur l'origine de la guerre, est cité en particulier : LINDEMANN Thomas « Les guerres américaines dans l'après-guerre froide : entre intérêt national et affirmation identitaire ». *Raisons politiques*, 13 (1), 2004, pp . 37-57.

¹²³ Notamment les travaux sur la démocratie qui font intervenir les analyses quantitatives et les analyses interprétatives avec l'héritage de Ludwig Wittgenstein. WEEDEN Lisa, « Concepts and commitments in the study of democracy », In. SHAPIRO Ian, SMITH Rogers M., and MASOUD Tarek E. (dir.), *Problems and Methods in the Study of Politics*, Cambridge University Press, 2004. pp. 274 – 306.

¹²⁴ Les causes « matérielles » et « formelles » (à l'intérieur du phénomène causé et qui en constituent l'essence et la substance), les causes « efficientes » (« motrices ») et « finales » (les raisons qui font qu'un évènement survient et son but, à l'extérieur du phénomène).

¹²⁵Voir KURKI Milja, *Causation in International Relations: Reclaiming Causal Analysis*, Cambridge Studies in International Relations, Cambridge University Press, avril 2008, 370 p. ainsi que KURKI Milja et WIGHT Colin, « International Relations and Social Science (Third Edition) ». In. DUNNE Timothy, KURKI Milja et SMITH Steve (dir.), *International Relations Theory: Discipline and Diversity*, Oxford University Press, 3^{ème} édition, 2013, pp 14-35.

pertinente », ni « contextuellement non pertinente »¹²⁶. Ces catégories ne sont pas exclusives. Les explications dites « fausses » peuvent l'être pour deux raisons¹²⁷. Soit, elles sont factuellement fausses en ce sens qu'elles pourraient constituer une explication si elles avaient été vraies. Soit, elles sont fausses car elles acceptent les présupposés faux d'une question. Autrement dit, répondre à une question fausse invalide l'explication donnée. Les explications « objectivement non-pertinentes » n'ont pas le caractère d'explication en tant que telles, même si elles sont factuellement vérifiables. Une explication doit porter sur le phénomène qu'elle vise à expliquer, faute de quoi elle ne constitue pas une explication. Enfin, les explications « contextuellement non pertinente » quant à elles indiquent que des explications ne sont bonnes que dans un certain contexte de recherche propre à l'analyse conduite et donc à l'intérêt du chercheur. Trois raisons peuvent justifier cette non-pertinence : l'explication répond à la mauvaise question, le destinataire n'est pas en mesure de comprendre l'explication, ou l'explication contient trop d'informations¹²⁸. Le caractère non-fermé de l'analyse constitue enfin une conséquence des biais, de la part d'arbitraire ou d'inconnus qui peuvent exister lors de cette sélection (voir Fig. 1). L'absence de lien construit entre les deux concepts s'expliquent d'après l'auteur par la proximité de la naissance de ces deux outils. Sur le caractère compatible de ses outils, il affirme leur nécessaire complémentarité :

« Le premier fournit le but idéal de la connaissance scientifique, alors que la seconde explique en quoi une explication donnée est explicative. Parce que ces deux questions sont différentes, les deux approches sont compatibles, et représentent deux aspects de l'analyse des explications. [...] l'érotétique est indispensable pour compléter les analyses de Raiton pour deux raisons. D'une part, elle indique pourquoi les éléments du texte explicatif idéal expliquent le phénomène étudié : - « ils font partie des réponses adéquates à des questions contrastives portant sur ce phénomène ». D'autre part, elle aide à identifier les « principes qui président au choix des informations explicatives », ce qu'« en pratique, seule l'érotétique peut faire» »¹²⁹

C'est en s'inscrivant dans ce cadre conceptuel et épistémologique que peut commencer à s'envisager la réponse à notre problématique sous l'angle des théories des Relations

¹²⁶ Jérémie Cornut reprend la typologie de Hällsten qu'il enrichit des écrits de De Langhe, Weber, Van Bouwel (précités) ainsi qu'une nouvelle lecture de Garfinkel (précité). HÄLLSTEN Henrik, *Explanation and Deduction: A Defence of Deductive Chauvinism*. Coronet Books Inc, 2001, 165 p. Et également : HÄLLSTEN Henrik, «What to ask of an explanation-theory ». In PERSSON et PETRI (dir.), 2007, op-cit., pp. 13-26.

¹²⁷ YLIKOSKI, 2007, op-cit. pp 32 – 34.

¹²⁸ Ibid.

¹²⁹ CORNUT, op-cit. pp. 174 - 175

Internationales. Néanmoins, considérant l'hypothèse et l'objet de recherche, ce premier pilier devra être complété par les théories de la sécurité et des analyses de discours.

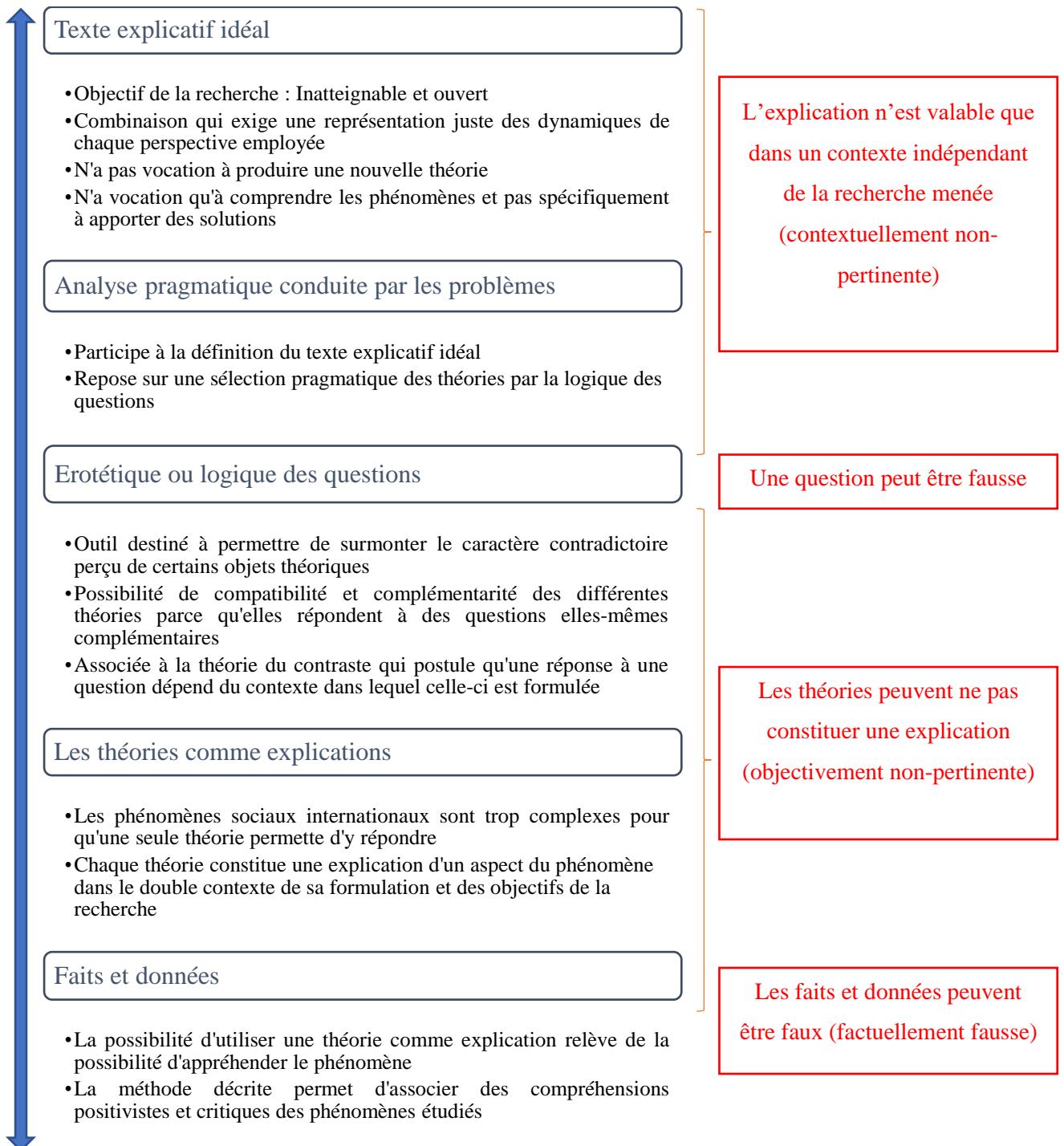


Figure 1 – Résumé des outils du pragmatisme conduit par les problèmes et des causes de non-pertinence des explications.

Section 2 – Les mots et les discours : De l'efficacité politique du langage à l'objectivation rhétorique du politique.

« Repartons de l'analyse du texte et du statut autonome que nous lui avons reconnu par rapport à la parole et à l'échange de paroles. Ce que nous avons appelé l'occultation du monde ambiant par le quasi-monde des textes engendre deux possibilités. Nous pouvons en tant que lecteur, rester dans le suspens du texte, le traiter comme texte sans monde et sans auteur ; alors nous l'expliquons par ses rapports internes, par sa structure. Ou bien nous pouvons lever le suspens du texte,achever le texte en paroles, le restituant à la communication vivante ; alors nous l'interprétons. Ces deux possibilités appartiennent toutes les deux à la lecture et la lecture est la dialectique de ces deux attitudes. »

Paul Ricœur¹³⁰

L'essentiel des approches politiques du langage ont en commun d'avoir pour point d'origine un doute sur le rapport entre le langage et la réalité. Hérité de la philosophie ce doute pourrait se résumer à : le langage a-t-il du pouvoir ? Ou plus précisément, comment comprendre l'efficacité politique du langage ?¹³¹ La Science Politique s'intéresse initialement au langage, non pas forcément pour lui-même, mais surtout car il influence l'exercice du pouvoir politique (et les représentations sociales)¹³². En effet, la conception aristotélicienne définit un exercice du pouvoir conduit par l'argumentation dont les règles permettent de persuader autrui. Mais plus encore, les premiers matériaux de travail de ces disciplines sont souvent des textes écrits ou des discours. Ces premiers écrits sont d'abord ceux des princes,

¹³⁰ Cette citation est issue du début de la partie dédiée à l'explication structurale du texte de l'œuvre de Paul Ricœur dédiée à l'herméneutique, *Du texte à l'action* (III – Le texte et l'explication structurale), où il dépeint l'analyse du texte au travers d'une approche construite sur la structure qu'il rapporte à la linguistique et à l'anthropologie structurale et qui fournit un modèle d'explication d'un texte entendu au sens de la présente citation. Autrement dit, le texte établit une césure (« occultation ») entre lui-même et son auteur. Chez Paul Ricœur, la distinction entre l'explication et l'interprétation du texte décrit un rapport au contexte du texte. RICŒUR Paul, *Du texte à l'action, Essais d'herméneutique II*, Paris, Seuil, 1996, 416 p.

¹³¹ Il existe de nombreux autres questionnements philosophiques liés au langage ayant trait à son origine, ses relations à la réalité, à la pensée, au sujet, à la raison ou encore à la connaissance... Le langage se trouve également dans un certain nombres d'autres objets que sont la communication, la langue, le texte, le signe. De fait, cette recherche se positionne au-delà du problème de la signification, soit : « comment un terme (ou signe) peut-il acquérir la signification du référent ? ». Sur la distinction entre discours et langage : CHARAUDEAU Patrick *Langage et discours, Éléments de sémiolinguistique*, Paris, Hachette Université, Coll. Langue, Linguistique, Communication, 1983, 176 p. Du même auteur : *Le discours politique. Les masques du pouvoir*, Paris, Vuibert, 2005, 256 p.

¹³² BOURDIEU Pierre, « Décrire et prescrire. Les conditions de possibilités et les limites de l'action politique », *Ce que parler veut dire. L'économie des échanges linguistiques*, Paris, Fayard, 1982, pp. 149-161.

puis ceux des auteurs, des normes et des théories scientifiques, des opinions, des récits ou encore des images et des symboles... Elément efficace du langage, le discours opère une articulation d'idées à travers moyens de diffusion. Le discours ne peut être un objet de recherche pour lui-même mais doit s'appréhender comme la manifestation d'une réalité sociale à laquelle on peut accéder par son analyse. Le périmètre de la notion de discours permet ainsi de considérer la matérialité discursive de plusieurs sources y compris en dehors du champ politique proprement dit¹³³. L'objet discours peut être caractérisé dans un texte, une prise de parole, une image, une œuvre d'art qui sont autant de moyens pour sa diffusion... L'analyse du discours en tant que telle se développe à partir des années 50 dans le monde académique, notamment avec le développement de la première chaire de lexicométrie à Saint Cloud, mais également par la sémiologie et l'étude des mythes dans la publicité de Roland Barthes¹³⁴. L'analyse du discours a également formé la base de la sociolinguistique...

D'un point de vue ontologique, la conceptualisation du discours peut se comprendre de deux manières : soit, il est une source du savoir et doit alors se comprendre à l'aide d'une analyse traditionnelle, soit, il doit être compris en tant que tel comme un processus qu'il faut analyser¹³⁵. Cela conduit l'analyse du discours à se positionner méthodologiquement au carrefour de deux logiques distinctes : d'une part, une démarche interprétative plutôt centrée sur le *logos* et la compréhension de la réalité derrière les mots ; d'autre part, une démarche explicative centrée sur les règles de formation et de transformation du discours.

La première tradition relèverait ainsi davantage des sciences sociales entendues au sens large, tandis que la seconde correspondrait davantage à l'apport des sciences

¹³³ Sur l'ouverture du champ politique aux éléments exogènes. Voir notamment : LE BART Christian, « L'analyse du discours politique : de la théorie des champs à la sociologie de la grandeur », *Mots. Les langages du politique*, 72, 2003.

¹³⁴ BARTHES Roland (1957), *Mythologies*, Paris, Le Seuil, 2015, 207 p.

¹³⁵ L'analyse du discours fait appel à un vaste ensemble de conceptualisations nées dans plusieurs disciplines scientifiques telle la psychologie, la sociologie, la linguistique, l'histoire... Il s'agit ici d'une typologie volontairement généraliste.

linguistiques¹³⁶... En tenant compte de cette grande division, la question est donc de savoir à quel point le sens qui émerge des pratiques discursives est influencé par leur caractère formel. Cette question trouve un sens particulier concernant les textes à vocation politique où les règles internes présidant la fabrique du discours sont tout aussi importantes que le contexte dans lequel ces textes s'inscrivent. Toutefois, cette division donne une vision tronquée de l'apport de la Science Politique dont elle ne permet pas de rendre compte de l'ensemble des approches. Aussi plutôt que l'étude l'ensemble des conditions de la production et de la reproduction des rapports sociaux, il faudrait se concentrer sur les phénomènes d'intersubjectivité en tant qu'ils sont médiatisés par le langage¹³⁷ combiné avec l'approche pragmatique évoquée en premier lieu. Cette approche ainsi teintée de réalisme critique ne peut ni faire l'économie d'une étude du contenu du discours, ni de l'économie du contexte et des conditions sociohistoriques de sa production.

Cette section reviendra sur la pluralité épistémique des cadres qui permettent de penser le discours en Relations Internationales en mettant en avant le lien entre philosophie, discours, sociologie et langage. Après avoir pris en compte, la pluralité des cadres théoriques qui fondent l'étude du discours en Relations Internationales et quelques-uns de ses développements (A), nous nous attarderons sur l'apport des études de sécurité (B), avant d'examiner des outils qui serviront d'une part à saisir la pluralité de sens et formes de l'objet « cyber » en tant que discours (C)

¹³⁶ Ces développements s'ils évoquent plus qu'ils n'abordent les conceptions de production et mutation du langage ne sauraient toutefois passer sous silence l'apport de la lecture des œuvres de Noam Chomsky. Sont tout particulièrement concernées sur ce point les œuvres CHOMSKY Noam, *Sur la nature et le langage*, Éditions Agone, coll. « Banc d'essais », 2011, 224 p et A ce titre, il faut également retenir le débat entre Michel Foucault et Noam Chomsky en 1971, retrancrit notamment dans l'ouvrage CHOMSKY Noam et FOUCAULT Michel, *Sur la nature humaine, comprendre le pouvoir, interlude*. Editions Aden, Bruxelles, octobre 2005, 200 p., (pp 7 – 87).

¹³⁷ On retrouve ici l'opposition entre un « paradigme de la production » et un « paradigme du langage » théorisée en sociologie par Gyorgy Markus qui ne se réduit pas à une simple opposition entre matérialisme et idéalisme (même si, notre objet le « cyber » implique la prédominance d'une pensée d'inspiration matérialiste) MARKUS, Gyorgy, *Langage et production*, Paris, Denoël, 1982, 222 p. Voir également les travaux de Jean Duchastel, et notamment pour l'application de cette théorie à l'analyse de discours ainsi que sur la distinction entre l'école « française » et l'école « anglo-germanique » et entre discours et analyse de contenu : DUCHASTEL Jean « Discours et informatique : des objets sociologiques ? », *Sociologie et sociétés* 252, 1993, pp. 157–170.

A – Penser le discours comme objet politique pour les Relations Internationales : une mosaïque de théories, d’outils et de postures.

La compréhension académique du discours dans les Relations Internationales existe en filigrane dans l’histoire de la discipline à partir du moment où les idées, les valeurs et les doctrines sont des déterminants admis des relations extérieures des États. La conceptualisation du discours comme objet d’étude à part entière est souvent considérée un peu vite comme la spécificité des approches « critiques » ou/et « radicales » des Relations Internationales. Toutefois, cet objet du discours ne doit pas être compris comme un « objet nouveau »¹³⁸. Cette insertion du discours dans la discipline s’opère par les liens profonds qu’elle entretient avec la Philosophie politique et l’Histoire des idées. L’aspect discursif des matériaux textuels de la Science Politique qualifie un certain nombre d’approches visant l’étude de ces mêmes textes : en particulier les méthodes issues de la Philosophie politique. Sous ce prisme le discours peut être compris comme le reflet de la pensée d’un auteur, le produit des intérêts socio-économiques de celui-ci, ou la traduction d’un contexte intellectuel particulier qui varie en fonction de l’intention de l’auteur. Ainsi, Alice Baillat, Fabien Emprin et Frédéric Ramel¹³⁹ identifient la méthode exégétique dite classique, la méthode analogique dite « marxiste » puis « critique d’inspiration néomarxiste », et la méthode historique de l’école de Cambridge. L’exégèse qu’ils rapportent aux travaux de Léo Strauss se fonde sur une méthode double dans l’analyse du texte des « grands auteurs » tels Machiavel, Hobbes ou Rousseau. La première composante « exégétique » se rapporte à l’étude des concepts et des procédés généraux de la pensée de l’auteur. La seconde composante est de nature « ésotérique » comprise au sens de mystique, c’est-à-dire le sens caché du texte (ce qui a été dissimulé par l’auteur à raison du contexte de l’écriture). La méthode de l’analogie quant à elle suppose une « correspondance étroite entre le contenu des textes [politiques] étudiés et la structure sociale et économique au moment de leur rédaction ». Les exemples cités sont les travaux sur les *Federalist papers* de

¹³⁸ Voir notamment MILLIKEN Jennifer. « The Study of Discourse in International Relations:: A Critique of Research and Methods. » *European Journal of International Relations*, vol. 5, no. 2, Juin 1999, pp. 225–254,

¹³⁹ Il s’agit d’une revue méthodologique pour un étude des discours sur l’État de l’union du Président G.W. Bush et B. Obama. BAILLAT Alice, EMPRIN Fabien, RAMEL Frédéric, « Chapitre 12 - Des mots et des discours. Du quantitatif au qualitatif », In. DEVIN Guillaume (dir.) *Méthodes de recherche en relations internationales*. Paris, Presses de Sciences Po, « Relations internationales », 2016, p. 227-246.

Charles Beard¹⁴⁰ et les travaux sur la domination de Robert Cox en Relations Internationales¹⁴¹. La dernière méthode évoquée, historique, repose sur le repérage des conventions et l'intentionnalité de l'auteur afin de les situer en tant qu'acte dans l'histoire et le langage. L'exemple est celui des travaux sur Machiavel de Quentin Skinner¹⁴². Le but d'une telle approche est d'éviter la mise en relief d'une mythologie des idées à travers les écueils que sont l'anachronisme et la mauvaise interprétation de l'intentionnalité des auteurs. Pour compléter ce tour d'horizon de la méthode en lien avec le champ, plusieurs compléments nous semblent nécessaires pour intégrer le langage sous les prismes historiques, épistémologiques et tenir compte des liens construits entre la philosophie du langage et les Théories des Relations Internationales.

Le langage n'est pas compris par une sémantique de la langue, mais une sémantique de discours. Le langage y est perçu comme implicite : ce n'est pas tant son sens qui compte que la valeur attribuée dans son rapport avec son contexte d'énonciation et de réception quelle que soit la théorie qui fonde ledit contexte. Une compréhension critique discours s'opère généralement du fait de la réception dans le champ des Relations Internationales du « tournant linguistique »¹⁴³. Inspiré de la philosophie de Wittgenstein, ce postulat historiographique part du principe que toute analyse ne peut se faire sans une analyse préalable du langage. Cette réception du tournant linguistique a conduit au développement du langage compris comme une action. Le rôle de ces actes du langage consiste à mettre en avant l'illusion descriptive en se fondant sur le concept de performativité. Cette performativité formera le socle de la théorie des actes de langage qui appuiera plusieurs de ces développements liminaires. Développée par John Langshaw Austin dans son ouvrage *Quand dire c'est faire* publié en 1962, la « performativité » signifie l'atteinte du résultat recherché par sa seule énonciation. Ce concept est à la base de la théorie des actes de langage. A noter qu'Austin finira par abandonner ce concept au profit d'autres termes issus de la linguistique. Ce dernier fera alors l'objet de

¹⁴⁰ BEARD Charles (Macmillan, 1913), *An Economic Interpretation of the Constitution of the United States*, Courier Corporation, mars 2012, 336 p.

¹⁴¹ COX Robert W. et SINCLAIR Timothy J., *Approaches to World Order*, Cambridge, Cambridge University Press, 1996, 572 p.

¹⁴² SKINNER Quentin (1981), *Machiavel*, Paris, Le Seuil, coll. « Philosophie Générale », 1989, 181 p.

¹⁴³ Pour le domaine des Relations Internationales, il est associé à la publication de l'anthologie philosophique de Rorty : RIORTY Richard (1967), *The Linguistic Turn. Recent Essays in Philosophical Method*, The University of Chicago Press, 1992, 416 p.

réappropriations au sein des sciences sociales. La performativité a notamment été approfondie dans une approche constructiviste par John Searle¹⁴⁴ qui, reprenant les travaux de Peter L. Berger et Thomas Luckmann¹⁴⁵, applique le concept aux actes sociaux où la langue n'est finalement que le « symptôme » de la construction des réalités sociales¹⁴⁶. Il serait également intéressant de compléter l'approche en citant les travaux d'autres auteurs emprunts d'une méthode « historique » en reprenant les auteurs que Skinner envisage lui-même comme représentatifs du « scepticisme » à l'égard de « l'étude des textes » et de la possibilité de restituer à l'égard de la possibilité de restituer la signification de l'intention fondamentale des auteurs du passé : Roland Barthes, Michel Foucault et Jacques Derrida¹⁴⁷. Des travaux de Roland Barthes, les relations internationales pourraient tirer plusieurs concepts notamment « l'effet de réel » en combinaison avec le récit ou le mythe en tant que signe sans qu'il soit besoin d'un auteur : « Chaque objet du monde peut passer d'une existence fermée, muette, à un état oral, ouvert à l'appropriation de la société »¹⁴⁸. Les travaux construits sur une méthode « foucaldienne » reprennent l'idée d'immanence contenue dans le diptyque « savoir-pouvoir » de Michel Foucault ainsi qu'une méthode généalogique foucaldienne. Celle-ci se fonde sur le concept d'énoncé : soit un acte de discours accepté par les experts au sein d'un réseau d'actes du langage. Cette formation des concepts fonde une théorie de la connaissance axée sur les transformations à laquelle vient s'ajouter la démarche interprétative de la généalogie fondée sur le contexte qui détermine l'évolution des conditions de vérité du

¹⁴⁴ Lequel est entré dans une controverse philosophique importante avec Jacques Derrida autour de l'héritage d'Austin et des actes de langage. MOATI Raoul, *Derrida, Searle : Déconstruction et langage ordinaire*, Paris, PUF, coll. Philosophies, 2009, 153 p.

¹⁴⁵ BERGER et LUCKMANN, op-cit.

¹⁴⁶ SEARLE John R. *The Construction of Social Reality*, Simon and Schuster, 1995, 241 p.

¹⁴⁷ SKINNER Quentin, « Motives, Intentions and the Interpretation of Texts », *New Literary History*, vol. 3, n°2 (1972), p. 393-408.

¹⁴⁸ Voir notamment pour l'effet de réel : BARTHES Roland. « L'effet de réel ». In. *Communications*, « Recherches sémiologiques le vraisemblable »..11, 1968, pp. 84-89 ainsi que pour le mythe : *Mythologies*, Paris, Éditions du Seuil, 1957 - 267 p. | La citation est issue de la page 216.

discours¹⁴⁹. Nous reviendrons sur le concept d'*épistémè* au moment d'aborder le concept de communauté épistémique.

Il est enfin nécessaire de citer l'apport de Jacques Derrida à travers la « déconstruction ». Autrement dit, pour un texte donné de faire dépendre sa signification non pas du repentie des représentations issues du texte que du langage qui le compose. Cette déconstruction appliquée aux concepts qui inspirera l'étude sur l'anarchie réalisée par Richard Ashley. Dans cette étude fondatrice du « post-positivisme » en Relations Internationales, l'auteur décrit le concept comme un élément théorique justifiant la souveraineté régaliennes. Concept antithétique de la souveraineté, l'anarchie favorise le modèle de l'État souverain en tant que modèle régulateur¹⁵⁰.

L'apport du discours en Théories des Relations Internationales se comprend premièrement comme la critique d'elles-mêmes et de la « conversation scientifique » qui les entoure. Les développements antérieurs nous permettent ici de privilégier les autres formes de prise en compte du discours. D'un point de vue politique, cela se traduit par la prise en compte d'une efficacité du langage dans l'étude. Dans ces approches, les chercheurs internationalistes utilisent le discours pour qualifier les concepts principaux utilisés pour comprendre l'international ou employés par les acteurs eux-mêmes. En établissant un lien entre théories et discours, ces travaux soulignent que les concepts employés opèrent une justification d'un ordre établi excluant les autres propositions. Depuis la seconde moitié des années 90 avec le développement de l'institutionnalisme néolibéral, l'analyse porte sur les discours d'autres acteurs, notamment les organisations internationales. Le focus opéré par la recherche sur la question de la morale dans les Relations Internationales depuis les années 2000 fait des

¹⁴⁹ FOUCAULT Michel (1969), *Archéologie du savoir*, Paris, Gallimard, 2014, 294 p. Voir pour les relations internationales l'un des ouvrages les plus récents : BONDITTI Phillippe, BIGO Didier et GROS Frédéric, *Foucault and the Modern International, Silences and Legacies for the Study of World Politics*, New York, Palgrave, 2017, 376 p. Voir également DER DERIAN James, « Foucault et les Autres : rencontres critiques dans le domaine des relations internationales », *Revue internationale des sciences sociales*, 2007/1 (n° 191), p. 77-82. Ainsi que le chapitre : LA BRANCHE Stéphane. « L'apport de Foucault aux théories des relations internationales : une critique du postmodernisme anglo-saxon ». In. MEYET Sylvain, NAVES Marie-Cécile, et RIBEMONT Thomas; *Travailler avec Foucault. Retours sur le politique*, L'Harmattan, Cahiers Politiques, 2005, pp. 119-139.

¹⁵⁰ ASHLEY Richard K. « Untying the Sovereign State : A Double Reading of the Anarchy Problematique », *Millennium*, Vol 17, Issue 2, 1998, pp. 227 – 262.

organisations internationales et de leurs controverses un terrain privilégié de ce type d'analyse¹⁵¹. Conceptualisées comme des « machines anti-politiques »¹⁵², les organisations internationales (en particulier l'ONU) sont regardées comme une extraction des relations internationales du « champ politique » au profit d'une dimension experte, technique et bureaucratique. Cependant, le discours de légitimation de ces mêmes acteurs fondée sur la production de normes universalistes, de bonnes pratiques ou d'expertise n'en extrait pas le côté politique. De même que le refus de l'idéologie ou le refus de la religion sont respectivement des positions idéologique ou religieuse, un concept tel que celui de « développement » possède une existence et des effets dans le champ politique¹⁵³. Dans ces études, le discours est de nouveau retenu par rapport à une critique d'une action normative de l'acteur.

Il en va de même dans d'autres champs de la recherche, par exemple en sociologie des crises politiques qui mettent en avant au travers d'une certaine « plasticité » l'importance des différentes tactiques et perceptions des acteurs dans des contextes de crise. En 1987, l'étude menée par Michel Dobry met en avant un certain nombre de biais qui relèvent de l'étude des crises qu'ils qualifient d'« illusion »¹⁵⁴. D'une part, l'illusion étiologique qui rapporte l'étude du phénomène de la crise à sa causalité. D'autre part, à l'inverse, la mise en avant des processus et phases ayant conduit à un résultat est qualifiée d'illusion de l'histoire naturelle. Focalisé sur « l'effet », le principe de cette deuxième illusion est que le déchiffrement de la réalité procède l'ordonnancement séquentiel de régularités dans une historiographie finalisée. Enfin, il y a l'illusion héroïque qui qualifie l'idée que les crises et les révolutions s'opposent aux périodes ordinaires du fait de l'action d'un certain nombre d'individus et de groupes sans considérer l'enjeu systémique de la structure. Dans cette approche l'auteur s'oppose à une vision du fait discursif qui consisterait à en faire un élément purement idéal. Au contraire, Michel Dobry insiste sur le fait que les définitions des situations (« de crise »), des perceptions

¹⁵¹ PETITEVILLE Franck, « Les organisations internationales dépolitisent-elles les relations internationales ? », *Gouvernement et action publique*, 2016/3 (N° 3), pp. 113-129.

¹⁵² Reprenant l'expression employée par Birgit Müller (P. 12). MÜLLER Birgit, « Comment rendre le monde gouvernable sans le gouverner : les organisations internationales analysées par les anthropologues », *Critique internationale*, 54, pp. 9-18.

¹⁵³ Voir par exemple RIST Gilbert, (1996) *Le développement : histoire d'une croyance occidentale*, Paris, Presses de Sciences Po, coll. « Monde et sociétés », 4^e édition, 2013, 520 p.

¹⁵⁴ Voir notamment les chapitre 2 et 3 de l'ouvrage en sa troisième édition (pp. 45 – 124) : DOBRY Michel (1987). *Sociologie des crises politiques. La dynamique des mobilisations multisectorielles* Paris, Presses de Sciences Po, 3^{ème} édition, 2009, 432 p.

ou des anticipations émergent de compétitions qui ne se réduisent jamais à des idées tout en s’inscrivant dans une désectorisation tendancielle de l’espace social faisant écho à la plasticité de la « structure » des systèmes sociaux. Les éléments définissables au travers du discours sont façonnés et redéfinis par les échanges de coups entre les acteurs et les transformations affectant les structures des « jeux » dans lesquels ces acteurs « sont pris ». Ontologiquement, il n’existe pas plusieurs niveaux de réalité et celle-ci possède une existence qui dépasse les seules croyances ou perceptions des acteurs. Enfin et surtout, ces croyances, discours, valeurs et les identités des acteurs sont également façonnées par les événements et les actions des acteurs¹⁵⁵. A l’échelle des Relations Internationales, c’est dans le domaine des études consacrées à la sécurité que cette conceptualisation du discours a connu le plus d’échos¹⁵⁶.

B - Approches discursives de la sécurité : entre réalismes, constructivismes et poststructuralismes.

A l’instar de la Science Politique ou des Relations Internationales, la sécurité ne fait pas consensus¹⁵⁷. Les quelques définitions qui obtiennent le plus d’adhésion sont celles qui mettent en avant l’impossibilité de celui-ci. La première d’entre elles est formulée par Arnold Wolfers : La sécurité, dans un sens objectif, mesure l’absence de menaces envers les valeurs centrales (« *acquired values* ») d’un acteur, dans un sens subjectif, l’absence de peur que de telles valeurs soient attaquées¹⁵⁸. L’introduction de la dimension discursive de la sécurité commence dans ce champ d’étude précis avec l’élargissement du concept de sécurité. Cet élargissement est souhaité par l’auteur qui par cette définition remet en cause le discours de « l’intérêt national » et la « sécurité nationale » tenu aux États-Unis d’Amérique durant la guerre froide pour constituer un objectif commun dans la lutte contre l’Union soviétique¹⁵⁹.

¹⁵⁵ DOBRY, op-cit. Préface de l’édition de 2009, pp. XI – XLV.

¹⁵⁶ Domaine constitutif pour une partie des Relations Internationales. Voir notamment les chapitres 3 (pp. 165 – 250) et 4 (pp. 251 – 358) de l’ouvrage BALZACQ Thierry, *Théories de la sécurité, les approches critiques*, Paris, Presses de Science Po, 2016, 512 p.

¹⁵⁷ Elle est définie par Walter Bryce Gallie comme un « *essentially contested concept* » (concept essentiellement contesté). GALLIE Walter B. , « Essentially Contested Concepts », *Proceedings of the Aristotelian Society* vol. 56, 1955, pp .167 - 198.

¹⁵⁸ WOLFERS, Arnold, « National Security as an Ambiguous Symbol » In. WOLFERS, Arnold (Ed.): *Discord and collaboration. Essays on International Politics*, Baltimore: John Hopkins, University Press): pp 147 – 165

¹⁵⁹ Ce qui relève d’une mutation nouvelle de la sécurité dans le discours qui favorisait avant la Seconde guerre mondiale la sécurité économique des individus.

La sécurité désigne une valeur subjective dont la définition s'associe à une culture particulière et des choix politiques. Elle est toujours définie négativement car elle suppose une absence d'insécurité. La plupart des réceptions du discours adoptent ainsi une posture susceptible d'adopter le label « critique »¹⁶⁰ y compris dans « l'âge d'or des études de sécurité »¹⁶¹. Une question demeure : celle de l'objet de la critique. Aux fins de sa distinction, nous reprendrons la typologie de Thierry Balzacq entre les études traditionnelles et les études critiques¹⁶². Cette typologie peut également se dégager des différents travaux qui illustrent une forme de transition entre les études stratégiques et la sécurité¹⁶³. Le « socle des études traditionnelles »¹⁶⁴ que Thierry Balzacq rapproche de la stratégie est une catégorie essentialisée regroupant la littérature préscientifique, la stratégie, l'influence de certaines théories des Relations Internationales et de la philosophie du Droit et une épistémologie positiviste de la connaissance. Ces études traditionnelles ont trois caractères d'identification : la centralité de l'État, l'impératif de la force militaire et le positivisme. A l'image de la première interrogation de David Baldwin¹⁶⁵, Thierry Balzacq se demande pour qui la sécurité doit être assurée. La réponse des études traditionnelles est celle de la sécurité pour l'État ; là où une posture critique serait plus ouverte sur d'autres aspects de cette sécurité.

L'auteur fait référence aux théoriciens du contrat social (Hobbes, Rousseau) ainsi qu'à Adam Smith. Au niveau de ce monopole de la sécurité, un parallèle pourrait être établit avec les théories de l'État dans un sens plus large notamment le concept de monopole de la violence

¹⁶⁰ Pour une synthèse sur les différentes typologies des « critiques » dans les études de sécurité : « redéfinir l'objet des études de sécurité », « se questionner et déconstruire les discours et savoirs en matière de sécurité », « contester la doxa sécuritaire », voir notamment : SIMONNEAU Damien, « Regard critique sur le label 'études critiques de sécurité' », *Études critiques de sécurité*. Vol. 46, N° 2-3, juin–septembre 2015.

¹⁶¹ L'expression provient de Stephen Walt par opposition avec un « âge de la renaissance » des études de sécurité dans les années 70. Il n'existe cependant pas d'historiographie satisfaisante des études de sécurité. L'article de Stephen Walt fut l'objet de nombreuses critiques. WALT Stephen M. « The Renaissance of Security studies », *International Studies Quarterly*, 35 (2), 1991, pp. 211-239.

¹⁶² BALZACQ, 2016, op-cit. pp 25-39.

¹⁶³ Notamment les travaux de Michael Williams et Keith Krause notamment : KRAUSE Keith et WILLIAMS, Michael C. « From Strategy to Security: Foundations of Critical Security Studies », In KRAUSE Keith et WILLIAMS, Michael C. (eds) *Critical Security Studies*, Minneapolis: University of Minnesota Press, 1997, pp. 33-59.

¹⁶⁴ BALZACQ, 2016, op-cit. p. 27.

¹⁶⁵ L'apport de David Baldwin réside dans une décomposition du concept de sécurité à l'aide de différentes questions : Pour qui assurer la sécurité ? Pour quelles valeurs ? Pour quel degré de sécurité ? Face à quel type de menace ? Avec quels moyens ? À quel prix et sur quelle période ? BALDWIN David, « The Concept of Security », *Review of International Studies*, vol. 23, n°1, 1997, pp. 5-26.

(*Gewaltmonopol*) de Max Weber en tant que définition sociologique de l'État¹⁶⁶. Un deuxième parallèle pourrait être construit avec monopolisation de la contrainte comme structurant le phénomène de civilisation dans la sociologie processuelle de Norbert Elias¹⁶⁷. Ces parallèles se justifient d'autant plus que le stato-centrisme des études traditionnelles se fonde sur l'empirie (l'État est l'acteur principal des Relations Internationales donc de la sécurité), mais également sur une dimension normative puisque l'État doit avoir une « valeur suprême » dans la hiérarchie des acteurs. L'impératif de la force militaire est consacré comme l'élément structurant des études stratégiques. La guerre est la principale menace pour les États et les menaces non-militaires n'appartiennent pas au champ des études de sécurité ou (en fonction des auteurs) sont considérées comme moins prioritaires. Enfin, le positivisme désigne un état de la connaissance scientifique qui obéit aux exigences de naturalisme¹⁶⁸, d'objectivisme¹⁶⁹ et de neutralité axiologique¹⁷⁰. Cette typologie du positivisme, elle-même inspirée des travaux de Mark A. Neufeld et la distinction du positivisme « comtien » (« *comtean* ») au profit d'une acception « logique » de celui-ci fondée sur une emphase de la logique symbolique qui permet de mettre en avant trois critères fondamentaux : le sens comme référentiel et l'importance du langage scientifique empirique comme son seul garant, l'utilisation d'un modèle nomologique fondé sur la déduction logique et la théorisation par la démarche hypothético-déductive¹⁷¹.

¹⁶⁶ WEBER Max (1959), *Le savant et le politique*, La découverte, 2003, 206 p.

¹⁶⁷ Le monopole de la violence est ici doublé du monopole fiscal. Voir l'ouvrage de 1939, *Sur le processus de civilisation* notamment la seconde partie : ELIAS Norbert (1975) *La dynamique de l'occident*, Pocket, coll. Agora, 2003, 320 p.

¹⁶⁸ Naturalisme au sens de la philosophie des sciences : la règle voulant que les techniques puissent accumuler de la connaissance par l'expérience notamment par l'unité de la méthode scientifique et des logiques de conjecture et de réfutation de Karl Popper, tout en visant une connaissance nomologique. Voir : POPPER Karl (1963), *Conjectures et réfutations : la croissance du savoir scientifique*, Payot, 2006, 610 p.

¹⁶⁹ Objectivisme : le monde réel existe et préside à la distinction entre la vérité et le mensonge : « la vérité ou la fausseté d'une proposition dérive de son degré de correspondance avec le monde réel » DAHL Robert, *Modern Political Analysis*, Englewood Cliff, Prentice Hall, 1963, p. 8, cité par BALZACQ, op-cit p. 37 (note 42).

¹⁷⁰ Le domaine de la connaissance scientifique est celui des faits, et non pas des normes ou des valeurs, et donc la connaissance scientifique (faits) est extérieure à la personne du chercheur (valeurs). Thierry Balzacq se fonde ici sur la distinction d'Horkheimer, domaine de la connaissance/domaine de l'action. HORKHEIMER Max, *Critical Theroy : Selected Essays*, New York, Seabury Press, 1972, p. 208. Cité par BALZACQ Thierry, Ibid (note 43).

¹⁷¹ Voir notamment le chapitre 2 (pp. 22 à 38) de l'ouvrage : NEUFELD Mark, *The Restructuring of International Relations Theory*, Cambridge, Cambridge university Press, 1995, 174 p.

Toute étude de sécurité qui s'éloigne de ces caractères peut être considérée comme entrant dans la catégorie des études critiques¹⁷². Le label « critique » ne se résume donc pas nécessairement à la théorie critique, mais trouve sa consécration dans quatre postures¹⁷³ : une posture ontologique cherchant à enrichir et dépasser à la sécurité de l'État ainsi que la réponse aux menaces par des moyens militaires ; une posture épistémologique impliquant la remise en cause de la constitution et de la production des savoirs académiques en ce qu'il légitime les politiques de sécurité ; une autre posture épistémologique qui questionne les protocoles de recherche et les conditions des contestations des politiques de sécurité ; et enfin la sociologie des sciences appliquée à la discipline qui considère avant tout l'idée critique comme le fruit d'une volonté de promotion de la part des chercheurs revendiquant le label¹⁷⁴.

1 – Le discours et l’élargissement du concept de sécurité : de la théorie critique aux constructivismes.

Vis-à-vis de la sécurité, le discours se conçoit en premier lieu comme un objet destiné à être critiqué par l'étude. Cette volonté qui sert la transition des études stratégiques vers les études de sécurité, prend forme lors de la définition d'Arnold Wolfers ainsi qu'avec les premières études critiques revendiquées.

Parmi les chercheurs de l'Ecole de Frankfort, le discours s'inscrit dans la conversation scientifique comme un objectif préparatoire à l'action nourrit par une démarche interdisciplinaire. Chez Max Horkheimer il n'existe pas de théorie de la société qui soit indépendante d'intérêts politiques et puisse conduire à une réflexion neutre dépourvue de toute référence à son contexte historique¹⁷⁵. De fait, la théorie est le reflet de la société dans laquelle émerge et se positionne contre l'ordre établit : elle est un discours de contestation. Le terrain de prédilection des tardives et premières études critiques appliquées à la sécurité est la sécurité

¹⁷² L'opposition n'est pas systématique aux dires de l'auteur. Prenant l'exemple de l'Ecole de Copenhague, il dit qu'elle est à la fois traditionnelle en affirmant la primauté de l'État et que la sécurité fonde tout problème sur une « logique de guerre », mais qu'elle est également critique lorsqu'elle accorde une force « pragmatique » au langage et reconnaît à la sécurité le pouvoir d'ordonner les priorités sociales et de « distribuer les positions sociales ». BALZACQ, 2016, op-cit. p. 51.

¹⁷³ Thierry Balzacq distingue quant-à-lui trois dimensions de la critique : « conceptuelle », « ontologique » et « épistémologique ».

¹⁷⁴ Par exemple : MUTIMER David, « Critical Security Studies: A Schismatic History » In COLLINS Alan, *Contemporary Security Studies*. Oxford: Oxford University Press, 3^{ème} édition, décembre 2010, pp 53 – 74.

¹⁷⁵ HORKHEIMER Max, *Théorie traditionnelle et Théorie critique*, Paris, Gallimard, 324 p.

nationale qui est critiquée à travers la sécurité des individus. La sécurité est présente indirectement dans la théorie critique car sa trame repose sur l'idée des appareils agressifs des États totalitaires (qui entravent le bonheur des individus). Plus largement, les approches critiques de la sécurité bénéficieront de l'apport des travaux critiques sur le discours bien que ces études ne fassent pas directement référence à la sécurité en tant que concept.

« Notre travail est nos mots, mais nos mots ne fonctionnent plus. Ils n'ont plus fonctionné depuis quelque temps. » [...] « Ces [concepts] et les autres concepts clefs, ne sont pas des mots de confiance avec lesquels aller à la théorétique chasse au tigre ».¹⁷⁶

La critique du lexique des Relations Internationales est le point de départ du travail de Ken Booth dans son article « Security and Emancipation » de 1991. La sécurité ne peut être appréhendée en des termes étatiques et militaires :

« Pour la plupart cependant, les menaces envers le bien-être des individus et des intérêts des nations ne découlent principalement des armées voisines, mais d'autres défis comme une crise économique, une oppression politique, une pénurie, la surpopulation, des rivalités ethniques, la destruction de la nature, le terrorisme, le crime, la maladie.[...] La plupart des êtres humains est davantage menacée par les politiques et insuffisances de leurs propres gouvernements que par les ambitions napoléoniennes de leurs voisins. »¹⁷⁷

Le langage s'implique ici à quatre niveaux particuliers dans la démonstration : le lexique des Relations Internationales, la conversation scientifique centrée autour d'une critique d'une vision réaliste de la sécurité, l'historiographie et la finalité pédagogique de cette dernière. L'approche défendue par Ken Booth part d'une émancipation qui fonde une sécurité individuelle contestant la puissance et l'ordre¹⁷⁸. L'État n'est pas fiable comme référentiel pour la sécurité car la plupart des études sont basées sur la théorie de l'État et non sur la pratique. Pour l'auteur, la sécurité ne peut pas être favorisée en incluant en tant que référents

¹⁷⁶ Notre traduction. Les concepts auxquels il est fait référence sont souveraineté, États, superpuissances, guerre, stratégie et armes. Extraits de l'introduction « words problems and world problems » de l'article BOOTH Ken. « Security and Emancipation. » *Review of International Studies*, vol. 17, no. 4, 1991, pp. 313–326.

¹⁷⁷ Ibid. p. 318. Sur les développements de ces enjeux autres que militaires, voir également le chapitre 4 (pp. 93 – 124) de l'ouvrage WYN JONES Richard, *Security, Strategy, and Critical Theory*, Lynne Rienner Publishers, 1999, 191 p.

¹⁷⁸ Une partie des développements de l'auteur fait référence aux travaux d'Hedley Bull. Voir : BULL Hedley, *Justice in International Relations*, University of Waterloo, Hagey Lectures, 1983. L'idée d'émancipation formera également l'un des concepts de ses travaux ultérieurs. Notamment, le chapitre 3, « Security emancipation community » de l'ouvrage BOOTH Ken, *Theory of World Security*, Cambridge University Press, 2007, 516 p.

théoriques et pratiques tous les régimes étatiques notamment ceux avec des dirigeants tels que Saddam Hussein, Hitler ou Staline. L'auteur reproche également la confusion de la fin et des moyens. L'État n'est que le moyen. Il est donc illogique de privilégier sa sécurité par rapports à la sécurité des fins (le bien-être de la population). Enfin, reprenant l'idée d'un mauvais positionnement de la théorie de l'État¹⁷⁹, Ken Booth affirme que l'État ne peut servir de base tant ses caractéristiques peuvent varier dans le temps et les époques : il est par exemple impossible pour les États-Unis d'Amérique et Tuvalu de constituer à ses yeux une base commune d'une étude du concept de sécurité.

Thierry Balzacq résume l'apport de la théorie critique à la sécurité à trois « positions directrices » : les dimensions sociologique, normative et praxéologique¹⁸⁰. La dimension sociologique repose sur une historiographie de la naissance de l'État et de la conception de la sécurité qui en découle¹⁸¹. La théorie critique envisage l'État comme une étape politique temporaire. La dimension normative complète la première dimension en affirmant que l'État représente un obstacle à l'émancipation¹⁸². Et enfin la praxéologie qui milite pour le développement d'alternatives sensibles à l'intérêt de l'émancipation¹⁸³. La dimension discursive se retrouve dans les critiques sociologiques et normatives adressées aux États. Celle-ci existe d'abord par le rôle important des idées. Robert Cox en fait la première des trois forces qui viennent influencer la configuration des structures historiques. Articulées par les « institutions » avec les « capacités matérielles », ces idées participent de la formation du cadre politique de l'action. Les idées sont de deux sortes : les conceptions communément admises sur la nature des relations sociales (« sens intersubjectif ») et les différentes conceptions permettant de comprendre les rapports de pouvoir et leur légitimité au sein de divers groupes (« images collectives »). La dimension normative mobilise les outils de l'éthique du discours afin de dégager deux obstacles à l'émancipation : la restriction de

¹⁷⁹ HELD David, « Central Perspectives on the Modern State », In. HELD David et al. (eds.), *States and Societies* Oxford, Martin Robertson, 1983, pp. 1 -55.

¹⁸⁰ BALZACQ, 2016, op-cit. pp. 97 – 112.

¹⁸¹ C'est l'occasion pour l'auteur de décrire la conception de Robert Cox en faisant notamment référence à l'article : COX Robert, « Social Forces, States, and World Orders », *Journal of International Studies*, 10 (2), juin 1981, p. 129.

¹⁸² L'auteur mobilise ici la seconde édition de 1990 de l'ouvrage : LINKLATER Andrew, *Men and Citizens in the Theory of International Relations*, Springer, 1982, 232 p.

¹⁸³ Voir notamment l'éthique de la discussion Habermas, cf. infra.

compétences et le particularisme éthique. La « restriction des compétences », définie par Jay M. Bernstein¹⁸⁴, illustre les catégorisations mises en place par des groupes dominants au sein de l’État qui créent des sources d’insécurité pour les groupes dominés. Le particularisme éthique¹⁸⁵ formulé par Andrew Linklater est le fruit de la logique étatique qui consacre une distinction entre « l’humain » et « le citoyen », ainsi qu’entre « l’interne » et « l’externe ». L’auteur met en avant une forme de déficit moral car « le citoyen » l’emporte sur « l’humain » et « l’interne » sur « l’externe ». Également tirée des outils développés par Jürgen Habermas, la dimension praxéologique érige le discours et le dialogue comme la forme des alternatives sensibles. Dans sa *Théorie de l’agir communicationnel*¹⁸⁶, oppose le « système » du marché et de la bureaucratie au « monde vécu » culturel et domaine de la compréhension intersubjective. Le premier empiète sur le second au travers d’un processus de bureaucratisation. Face à la rationalité instrumentale du système, Jürgen Habermas propose une émancipation fondée sur la communication qui fonde une compréhension mutuelle. Cette communication entretient un rapport particulier au langage qui dénote une rationalité fondée dans l’argumentation : soit les capacités à construire des arguments et à éprouver ceux-ci à travers la discussion. L’argumentation ne rend possible la compréhension que dans un contexte de non-violence (égalité et absence de répression), d’empathie (respect à l’égard d’autrui) et de jeu de rôle idéal (percevoir le monde à travers le point de vue de l’autre). Dans ces circonstances, l’argumentation s’entend du discours en tant qu’activité conduisant de façon réflexive par l’échanges d’arguments à la compréhension mutuelle¹⁸⁷.

Au-delà des questions liées à la sécurité individuelle, à la sécurité humaine ou au terrorisme, cet élargissement du concept de sécurité par le biais du discours est également un des apports du constructivisme aux études de sécurité. Sans nous attarder sur la question des typologies de constructivisme, nous retiendrons que le constructivisme désigne un ensemble d’approches où les interactions humaines sont façonnées par des facteurs idéels et non

¹⁸⁴ BERNSTEIN Jay M. (1995), *Recovering Ethical Life : Jürgen Habermas and the Future of Critical Theory*, Londres, Routledge, 2014, 264 p.

¹⁸⁵ LINKLATER, op-cit. pp.27 - 28.

¹⁸⁶ HABERMAS Jürgen (1981), *Théorie de l’agir communicationnel*, Volume 1, Rationalisé de l’agir et rationalisation de la société Paris, 1987, 448 p.

¹⁸⁷ Le questionnement autour de l’éthique du discours chez Jürgen Habermas revient à décider par le biais de l’argumentation de l’adoption de normes par une communauté humaine. HABERMAS Jürgen, *De l’éthique de la discussion*, Paris, Fayard 1999, 202 p.

seulement matériels. Les facteurs idéels les plus importants sont les croyances intersubjectives largement partagées, lesquelles ne sont pas réductibles aux individus. Ces dernières participent de la construction des intérêts et des identités des acteurs orientés vers un objectif¹⁸⁸. Le constructivisme est introduit dans les Relations Internationales par Nicholas Onuf¹⁸⁹ lequel influencé par la linguistique défend notamment le concept de langage performatif appliqué à la loi et l'ordre¹⁹⁰. Si d'un point de vue constructiviste, la sécurité est avant tout question de perception par les différents acteurs de menaces qui donnent sens à leur environnement, le discours et plus généralement le langage reçoivent différents statuts en fonction des chercheurs qui étudient la sécurité (selon que ceux-ci seront plutôt conventionnels ou critiques).

Des auteurs comme Alexander Wendt ou Peter J. Katzenstein ne consacrent aucune acceptation « systématique » du rôle du langage dans le constructivisme. D'autres auteurs, inspirés par des approches à dominantes linguistiques, à l'image de Nicholas Onuf, Barry Buzan ou Ole Weaver, ont une définition que ne laisse que peu de place au contexte d'énonciation au profit d'un discours limité à ses règles constitutives¹⁹¹. Derrière cette différence, Thierry Balzacq, reprenant les conclusions de Maja Zehfuss, évoque un obstacle de nature épistémologique. Le constructivisme conventionnel en faisant communiquer majoritairement l'acteur par des gestes s'assure de la traductibilité des principes constructivistes dans la théorie des jeux que mobilisent certains libéraux et les réalistes^{192 193}.

¹⁸⁸ Typologie des axiomes du constructivisme de Martha Finnemore et Kathryn Sikkink : FINNEMORE Martha, KATHERYN Sikkink, « TAKING STOCK: The Constructivist Research Program in International Relations and Comparative Politics », *Annual Review of Political Science*, 4:1, 2001, pp. 391-416

¹⁸⁹ ONUF Nicholas (1982), *World of our Making : Rules and Rule in Social Theory and International Relations*, Routledge, 2012, 340 p

¹⁹⁰ Ibid chapitre 2, pp 66 – 95.

¹⁹¹ BALZACQ, op-cit. note 90, p. 188 – 189.

¹⁹² ZEHFUSS Maja, « *Constructivisms in International Relations: Wendt, Onuf, and Kratochwil'* » In. FIERKE Karin M. et JØRGENSEN Knud Eric (eds), *Constructing International Relations: The Next Generation*, Londres, ME Sharpe, 2001, pp. 54 -75.

¹⁹³ Plus généralement, sur les différences entre ces courants autour de la sécurité : MACLEOD Alex, « Les études de sécurité : du constructivisme dominant au constructivisme critique », *Cultures & Conflits*, 54, 2004, pp.13-51.

2 – Langage, discours et approches poststructuralistes de la sécurité.

« Le poststructuralisme est une approche texto-centrée et, dans l'extrême, le monde est un texte ; une expérience personnelle, une manifestation politique, une élection, négocier un traité [...]. Même le discours est un texte »¹⁹⁴

Dans les approches poststructuralistes de la sécurité inspirées notamment par Michel Foucault et Jacques Derrida¹⁹⁵, le discours se comprend comme le lien du dytique pouvoir-connaissance. Plus précisément, le pouvoir repose sur la construction de la connaissance par le discours. Le pouvoir et les relations qu'il implique culminent par l'instauration d'un « régime de vérité » constitutif du sujet et qui détermine ce qui est constitué comme admis ou déviant¹⁹⁶. En tant que norme de comportement et d'action, le discours est la cible de travail des chercheurs poststructuralistes.

Chez Foucault, le discours prend corps dans une formation discursive, un contexte. « Autrement dit, le discours est une intervention historique, parmi d'autres, dans une formation discursive. En ce sens, l'histoire est une série de formations discursives discontinues, différenciées les unes des autres, sous au moins trois angles : au niveau des objets discursifs, de leurs relations et de leur opérationnalisation. Toute une méthode, prompte à encoder la trajectoire des formations discursives, se développe alors : Foucault, s'inspirant de Nietzsche, l'appelle « généalogie ». Il lui assigne un but précis : enregistrer la singularité des événements en dehors de toute finalité autonome »¹⁹⁷. Un discours dominant est en cela le fruit de relations de pouvoir particulière qui ne maintiennent qu'artificiellement leur unité avec le passé.

Ontologiquement, cela veut dire que la généalogie foucaldienne ne se concentre pas tant sur les phénomènes que sur ce qui les a rendus possibles. Epistémologiquement, tout

¹⁹⁴ ROSEAU Pauline, « Once Again into the Fray : International Relations Confronts the Humanities », *Millennium*, 19 (1), 1990, p. 48

¹⁹⁵ Sur la distinction entre poststructuralisme et postmodernisme et leur usage indifférencié dans les études de sécurité, voir BALZACQ, 2016, pp 252 – 254.

¹⁹⁶ Défini par Michel Foucault dans son cours au Collège de France, *Du gouvernement des vivants* en 1980. Pour son application aux études de sécurité, voir notamment : EDKIN Jenny, « Poststructuralism », In. GRIFFITHS Martin (ed.), *International Relations Theory for the Twenty-First Century*, Routledge, 2007, p. 92.

¹⁹⁷ BALZACQ, 2016, op-cit p. 283.

phénomène susceptible d'être étudié procède d'une perspective particulière, elle-même susceptible d'interprétation. La première tâche de l'observateur consiste à retrouver les rapports de forces qui en ont imposé une compréhension particulière au détriment d'autres perspectives et à décrire l'évolution de ces rapports de force afin de cerner la contingence d'un phénomène. Dans l'approche de Derrida, le texte et le monde sont le produit d'interprétations et ne peuvent être appréhendés que grâce à d'autres interprétations. Ce qui leur confère un statut proche. Le jeu entre les différents textes et leur influence sur la description de la réalité est nommée jeu intertextuel¹⁹⁸.

L'écriture joue un double rôle dans le cadre de la sécurité : elle permet à la fois de dépasser l'intention communicationnelle liée à la politique de sécurité et de tenir compte de la survenance de circonstances imprévues par le texte. Il est transcendant à son contexte de production. Deux outils textuels peuvent être mobilisés : la déconstruction et la double-lecture. La déconstruction consiste à confronter de manière critique et créative toutes les interprétations et acceptations politico-normatives imposées. La double-lecture consiste quant à elle à lire un « texte » une première fois en le suivant le plus loyalement possible et une seconde en se focalisant sur ses fragilités.¹⁹⁹ ²⁰⁰.

3 – Les théories de la « sécurisation » : des « classiques » aux « critiques ».

Si la sécurisation est le fait de rendre « plus sûr » un objet ou un espace donné, la sécurisation désigne quant à elle l'entreprise (essentiellement linguistique) qui transforme un enjeu en problème de sécurité²⁰¹. Le discours de sécurité opère en négatif une construction discursive de la menace. La théorie de la sécurisation est proposée par l'Ecole de Copenhague notamment à travers l'ouvrage publié par Barry Buzan, Ole Waever et Jaap de Wilde en 1998 *Security : a New Framework for analysis*²⁰². En qualifiant un enjeu de

¹⁹⁸ Voir DERRIDA Jacques, « Signature Events Context », *Glyph*, vol. 1 Baltimore (Md.), Johns Hopkins University Press, 1975 pp. 172 – 197. Ainsi que DERRIDA Jacques, *De la grammatologie*, Paris, Minuit, 1967, 448 p.

¹⁹⁹ Pour un exemple, voir l'étude sur l'anarchie dans les Théories des Relations Internationales réalisé par Richard Ashley a déjà citée. ASHLEY, 1998, op-cit.

²⁰⁰ BALZACQ, 2016, op-cit p. 288 – 301.

²⁰¹ BALZACQ, 2016, op-cit. p. 193.

²⁰² BUZAN Barry, WÆVER Ole et WILDE (DE) Jaap, *Security : a New Framework for analysis* Lynne Rienner Publishers, 1998, 239 p

« sécuritaire », l'auteur de cet acte de langage produit une structure commune de sens qui formule une menace de nature existentielle et les moyens nécessaires pour y répondre²⁰³. « En nommant un certain développement un problème de sécurité, l'État peut réclamer un droit spécial, droit qui sera toujours défini, en dernière analyse, par l'État et ses élites »²⁰⁴. La sécurité est ce que l'on croit qu'elle est et ce qu'on dit qu'elle est. Elle ne se consacre pas exclusivement aux questions militaires et n'importe quel enjeu peut être consacré comme un objet de sécurité. Elle doit être étudiée comme une pratique et comme un processus. Elle a des règles particulières distinctes de celle du champ politique. Son objet référent est enfin toujours une forme de collectivité.

Deux types de sécurité doivent alors être distinguées : la sécurité de l'État (compris au sens de l'appareil régaliens) qui intéresse cinq secteurs (militaire, politique, économie, environnement et société), et la sécurité collective de la population ou « sécurité sociétale ». Cette dernière se caractérise dans les conditions de reproduction autonomes des identités sociétales. Pour accomplir la sécurisation, trois dimensions sont essentielles à l'acteur : d'une part, la maîtrise interne de l'acte de langage par le biais d'une grammaire spécifique (objet menaçant, point de non-retour et solution possible) ; d'autre part, une position d'autorité et enfin, la facilité à établir un lien entre l'objet désigné et les objets habituellement considérés comme menaçants. Cette idée de sécurisation a de nombreux points communs avec la politisation²⁰⁵.

Bien qu'il souligne un développement autonome des deux domaines de recherche, Philippe Bourbeau évoque plusieurs points communs : la construction sociale admise de l'objet d'étude, subjective et processuelle. Elle peut être positive ou négative. Elle se situe dans un contexte où tous les agents ne sont pas égaux et opèrent dans un espace social sujet aux luttes de pouvoir. Ces agents sont dans l'impossibilité de reconnaître à eux seuls un enjeu et agissent par opportunité. Ce qui implique dans un cas comme l'autre, une approche

²⁰³ WÆVER Ole « Securitization and Desecuritization », In. LIPSCHUTZ Ronnie D. (ed.), *Security*, New York, Columbia University Press, 1995,

²⁰⁴ WÆVER Ole, op-cit, p. 54 traduction par MACLEOD, 2004, op-cit §53.

²⁰⁵ Processus de requalification des activités sociales les plus diverses, « requalification qui résulte d'un accord pratique entre des agents sociaux enclins, pour de multiples raisons, à transgresser ou à remettre en cause la différenciation des espaces d'activité » LAGROYE Jacques, « Les processus de politisation », In. LAGROYE Jacques (dir.), *La politisation*, Paris, Belin, 2003, p. 359-372

casuistique importante des enjeux²⁰⁶. Pour l'auteur la distinction s'opère sur un critère de finalité : la sécurité est une affaire de survie. Cette conception s'oppose à une vision plus fine de la sécurité telle que nous l'avons évoquée plus haut. Elle a néanmoins le mérite de souligner la porosité des concepts de la politisation et de sécurisation. Toutefois, le critère distinctif semble davantage être l'idée du domaine d'exception dans lequel existeraient les enjeux de sécurité. Plusieurs reproches ont été adressés à l'Ecole de Copenhague par les constructivistes critiques. Si la vision de la sécurité de l'Ecole de Copenhague impliquerait une forme de statocentrisme, les critiques les plus fortes seront adressées au concept de concept de sécurité sociétale.

Sur la critique de l'État comme objet principal de la sécurité, deux arguments ont été avancés dans une perspective sociologique. Formulé notamment par Didier Bigo et Jeff Huysmans, le premier argument met en exergue une perturbation de la distinction entre sécurité intérieure et sécurité extérieure. Les auteurs emploient l'idée de « champ de sécurité » soit un champ de pratiques sécuritaires autonome des autres pratiques qui rejette l'idée des cinq secteurs²⁰⁷. Avec le second argument, Bill McSweeney s'inscrit en faveur d'une conception étendue de « la sécurité qui tienne compte des besoins humains, qui comprenne les dimensions négatives et positives de la sécurité et qui mette l'accent sur la relation entre communautés, collectivités, États et individus comme source de sécurité ou d'insécurité »²⁰⁸. Ici, ce n'est plus l'État qui est l'objet ultime de la sécurité, mais l'individu.

En résumé, la critique de la sécurité sociétale se fonde également sur deux arguments principaux. Premièrement, le concept implique la définition d'une identité unique, objectiviste et unidimensionnelle. Ainsi, elle impliquerait une forme d'essentialisme identitaire qui ferait fi des prétentions d'identités concurrentes et niant le caractère plural et subjectif de l'identité. C'est donc une vision partielle sinon partiale qui est dénoncée par les critiques de l'Ecole de

²⁰⁶ Sur les liens entre politisation et sécurisation, voir : BOURBEAU Philippe, « Politisation et sécurisation des migrations internationales : une relation à définir », *Critique internationale*, 2013/4 (N° 61), p. 127-145.

²⁰⁷ BIGO Didier « L'Europe de la sécurité intérieure : penser autrement la sécurité ». In LE GLOANNEC Anne-Marie (ed.), *Entre Union et Nations : l'État en Europe*. Presses de Sciences Po. 1998. p. 55 - 90. Ainsi que HUYSMANS Jeff, « Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security », *Alternatives*, 27, supplément, 2002, pp 41 - 62.

²⁰⁸ Résumé de la définition de la sécurité de Bill McSweeney par Alex Macleod. MACLEOD, 2004, op-cit, §44. MCSWEENEY Bill, *Security, Identity and Interests. A Sociology of International Relations*, Cambridge, Cambridge University Press, 1999, p 203.

Copenhague aux premiers rangs desquels Didier Bigo et Bill McSweeney. En effet, pour le premier, il y a une forme de méconnaissance du sens sociologique de l'identité qui est un processus négatif dont la sécurisation ne concerne pas la survie mais l'intolérance à l'égard des différences et plus généralement du changement. Il y aurait dans ce postulat une compréhension partisane de la distinction entre intérieur et extérieur pour qui l'identité est une donnée. Didier Bigo défend une vision tirée d'une approche critique et donc l'impossibilité d'avoir une représentation « fixiste » des identités²⁰⁹. Chez Bill McSweeney, la critique reproche la méconnaissance du caractère processuel de l'identité constituée de négociations permanentes. La conception dénoncée est unidimensionnelle dans la mesure où elle postule que la sécurité sociétale est seulement une question d'identité²¹⁰. Deuxièmement, la sécurisation des identités interroge les chercheurs sur l'impact et le rôle de leur travail vis-à-vis de celle-ci. Le dilemme normatif d'écrire la sécurité comme le qualifie Hyusmans consiste à se demander comment travailler sur la sécurité de la société en réduisant le risque de sécurisation de celle-ci²¹¹. Par exemple, Didier Bigo met en avant l'approche américaine qui consiste à rapprocher sécurité intérieure et sécurité sociétale²¹².

Les deux critiques principales au concept de sécurisation tiennent finalement dans sa dimension sociologique trop peu prononcée et sa nature purement discursive. « La labellisation est toujours le produit d'un rapport de forces pour l'énoncé légitime » dans lequel les professionnels de la sécurité peuvent jouer un rôle important.²¹³ Reprenant la dialectique du bourgeois et du barbare autour de l'immigration, Didier Bigo affirme que « la sécurisation n'est donc pas que de l'ordre des pratiques discursives, même si elle y trouve son origine. Elle est de l'ordre des pratiques non discursives, des technologies à l'œuvre, des effets de pouvoir, des luttes et plus particulièrement des compétitions institutionnelles au sein du champ de la sécurité »²¹⁴.

²⁰⁹ BIGO, 1998, op-cit. pp. 71-72 et 83-84

²¹⁰ MCSWEENEY,, 1999, op-cit. pp. 70-77

²¹¹ HUYSMANS, op-cit.

²¹² BIGO Didier « When Two Become One: Internal and External Securitisations in Europe ». In KELSTRUP Morten WILLIAMS Michael Charles (eds), *International Relations Theory and The Politics of European Integration. Power, Security and Community*. Routledge. 2000, pp. 171 - 204.

²¹³ BIGO 1998, op-cit. p. 70-71

²¹⁴ BIGO Didier, « Sécurité et immigration : vers une gouvernementalité par l'inquiétude ? », *Cultures & Conflits*, 31-32, printemps-été 1998.

La sécurisation devient « l'opérateur de conversion » validant l'affrontement des rhétoriques politiques au sein du champ politique qui valorise ou dévalorise certaines menaces. Cet opérateur acquiert force de vérité par les professionnels de la gestion de la menace, en fonction des transformations de la violence qu'ils observent et de leurs intérêts en tant qu'institutions. Ce sont ces institutions de sécurité qui créent leur objet comme objet légitime de discours en y investissant des hommes, du temps de travail, des appareils statistiques, des routines qui donnent corps aux labellisations politiques. En 2001, Thierry Balzacq proposait de la sécurisation la définition opératoire suivante :

« Un assemblage articulé de pratiques à travers lesquelles des artefacts heuristiques (métaphores, instruments politiques, répertoires d'images, analogies, stéréotypes, émotions, etc.) sont contextuellement mobilisés par un acteur sécurisateur qui incite l'audience à construire un réseau cohérent d'implications (sensations, pensées et intuitions), à propos de la vulnérabilité critique d'un objet de référence, lequel s'ajuste aux raisons de choix et d'actions de l'acteur sécurisateur, en investissant le sujet de référence d'une aura menaçante, à un point tel qu'une politique ciblée va immédiatement être adoptée pour le bloquer. »²¹⁵

Dans cette définition, « l'acteur sécurisateur » est celui qui émet le discours de sécurité visant à présenter un enjeu comme tel au travers d'un mouvement sécuritisateur. Le « sujet de référence » représente l'entité menaçante et « l'objet de référence » la valeur menacée. Les trois derniers éléments sont l'audience/le public (récepteurs du discours), le contexte et enfin l'adoption de politiques distinctes (mais pas forcément exceptionnelles)²¹⁶. Cette définition présente deux avantages : elle neutralise l'idée de secteur contenue dans la théorie initiale et elle n'implique pas un caractère nécessairement exceptionnel des mesures adoptées. Ainsi formulée, la sécurisation est susceptible de recouvrir deux champs d'études, l'analyse de discours sur la menace et l'étude du processus politique de légitimation et de création de moyens de gérer la menace.

Dans un article plus récent sur la sécurisation introduisant un numéro de la revue *Etudes Internationales* consacré à la sécurisation²¹⁷, Thierry Balzacq parle de trois failles

²¹⁵ BALZACQ Thierry op-cit, 2016 p. 194, faisant référence à la définition qu'il a proposé dans BALZACQ Thierry, « A Theory of Securitization : Origins, Core Assumptions, and Variants », In. BALZACQ Thierry (ed.), *Securitization Theory : How Security Problems Emerge and Dissolve*, New York Routledge, 2001, p. 3.

²¹⁶ BALZACQ Thierry, « The Three Faces of Securitization: Political Agency, Audience and Context », *European Journal of International Relations*, vol. 11, 2005, pp. 171 – 201.

²¹⁷ BALZACQ Thierry. « Théories de la sécurisation, 1989-2018. » *Études internationales*, volume 49, numéro 1, hiver 2018, pp. 7–24.

particulières qui viennent affecter le(s) concept(s) du point de vue de la recherche. Elles tiennent premièrement au statut théorique de la sécurisation, ainsi qu'à son rapport au domaine de l'exception et enfin à la remise en cause de l'analyse de discours comme méthode principale d'analyse au profit de l'éclectisme méthodologique. S'il est vrai que la sécurisation est un cadre d'analyse qui admet le pluralisme théorique comme méthodologique, nous retiendrons la dilution du rapport à l'état d'exception qui considère la sécurité comme une « politique de l'extraordinaire »²¹⁸.

L'école de Copenhague entend cet état d'exception de deux manières. D'une part, elle peut effectivement désigner le domaine de la sécurisation qui consiste dans un « déplacement » hors des conditions de la « politique normale ». D'autre part, elle n'implique pas forcément d'adoption de mesure d'urgence puisque la seule évocation d'une menace existentielle de nature à justifier l'adoption éventuelle d'une mesure d'urgence constitue une sécurisation²¹⁹. Dès lors le caractère exceptionnel des mesures correctrices concernant un problème n'est pas un indicateur pertinent d'une différence de nature entre un problème de sécurité et un problème politique. Ce caractère illustre uniquement une différence de degré dans un processus de prise en compte du caractère existentiel de la menace.

La sécurisation décrit ainsi une transformation en enjeu de sécurité. Laquelle tend à expliquer les origines de la sécurité ainsi que les effets de celle-ci. Cette question de l'origine des normes est fondamentale dans le constructivisme qui place la norme comme le fondement du social. Reprenant la définition de la norme en tant que « prescription sociale » de Paul Kowert et Jeffrey Legro²²⁰, Thierry Balzacq entend souligner dans le constructivisme l'étude des rapports entre les normes et le comportement, l'identité ou l'intérêt des acteurs²²¹. Les processus d'émergence et de changement d'une norme sont mis en avant au travers d'une approche cyclique du développement historique de celle-ci : le « cycle de vie des normes ». Ce concept fait plus particulièrement référence aux travaux de Katheryn Sikkink et Martha

²¹⁸ KALYVAS Andréas *Democracy and the Politics of the Extraordinary: Max Weber, Carl Schmitt, and Hannah Arendt*. Cambridge: Cambridge University Press, 2008, 340 p.

²¹⁹ Pour ces deux significations. Voir le chapitre 2 « Security Analysis : Conceptual Apparatus » de l'ouvrage BUZAN Barry, WÆVER Ole et WILDE (DE) Jaap, op-cit. pp 21-48.

²²⁰ KOWERT Paul et LEGRO Jeffrey, « Norms, identity, and their limits : a theoretical reprise » In. KATZENSTEIN Peter (ed.) *The Culture of National Security : Norms and Identity in World Politics*, New York, Columbia University Press pp. 451–497.

²²¹ BALZACQ, 2016 op-cit. p 232.

Finnemore qui décrivent un cycle en trois étapes : émergence, cascade et internationalisation²²². L'émergence d'une norme traduit une volonté d'impulsion de la part d'acteurs « entrepreneurs de la norme » qui souhaitent poser le cadre d'un problème particulier. Cette phrase repose principalement sur la persuasion et consiste à emporter l'adhésion d'une part significative de l'audience visée (soit par rapport à seuil numérique, soit parce que la norme a été adoptée par l'ensemble des acteurs les plus pertinents). L'atteinte de cet état correspond au point culminant de la norme.

L'acceptation n'est pas le seul critère puisque le précédent par rapport au contexte historique et la cohérence interne de la norme proposée sont également des facteurs déterminants pour anticiper sa trajectoire. Lorsque le point culminant est atteint, la norme peut entrer en phase de cascade ou de percolation. Dans cette seconde étape, les acteurs convaincus (États, organisations internationales...) s'attacheront à convaincre les acteurs indécis ou résistants du bien-fondé de la norme. La persuasion s'accompagne désormais d'un nouvel arsenal que sont la socialisation, l'institutionnalisation ou encore la démonstration. Si la première phase avait pour ressorts de motivation l'altruisme, l'empathie et l'engagement, la motivation est devenue la légitimité, la réputation et l'estime de soi. Enfin, l'internationalisation investit la norme d'un caractère automatique sous le fait du Droit et de l'administration où l'institutionnalisation et l'habitude produise un modèle dont le ressort est la conformité. La causalité idéelle vient préciser ce modèle normatif en précisant que celle-ci peut dans ses effets à la fois être constitutive (elle est la condition de la possibilité de l'objet étudié) ou régulatrice (source de critères permettant la discrimination du « bien » et du « mal »)²²³. Cette décomposition vient enrichir le modèle de la sécurisation en lui offrant une porte vers une compréhension du temps long qui semble davantage concerné par le moment de la transition entre deux champs que par le processus à analyser dans la durée.

Dans cette recherche, le concept de sécurisation sera notamment mobilisé à partir de sa définition de Lene Hansen et Helen Nissenbaum. S'inscrivant dans la suite de l'Ecole de

²²²FINNEMORE Martha. et SIKKINK Katheryn « International norm dynamics and political change ». *International Organization* , 52(4), pp. 887–917. Le modèle sera porté plus loin avec les travaux de Wayne Sandholtz sur les alternances entre les phases du modèle. SANDHOLTZ Wayne, « Dynamics of International Norm Change: Rules against Wartime Plunder » *European Journal of International Relations*, Vol 14, Issue 1, mars 2008, pp. 101 - 131

²²³ Voir notamment BALZACQ, 2016, pp. 243 – 248. Pour notre part, nous nous focaliseront sur la compréhension de la cause déjà évoquée. Cf. KURKI 2008 op-cit.

Copenhague, leur article théorise la cybersécurité comme une forme de secteur distinct comportant ses propres menaces et ses objets de référence. Parmi les objets de références significatifs, la sécurité du réseau et la sécurité individuelle y jouent un rôle majeur du fait des connexions avec les objets de référence collectifs de l'État, de la société, de la nation et de l'économie²²⁴.

C – Epistémologie du discours chez Jean-Claude Passeron : comprendre la prolifération des mots dans et hors « la cité des sciences ».

Si le cadre développé jusqu'à présent répond à la question de savoir comment intégrer le phénomène étudié dans un ensemble plus large (les théories des Relations Internationales), elle ne permet pas nécessairement de décrire et délimiter les critères (étudier le phénomène). En effet, il ne traduit pas une composante fondamentale de l'empirie : la prolifération²²⁵. Autrement dit, s'il est possible d'inclure un objet définissable *a priori*²²⁶, la difficulté surgit quand le phénomène n'a pas de limite perceptible. Par prolifération, nous entendons la multiplication rapide des occurrences de l'usage des termes dérivés du cyberespace, sans qu'il soit réellement possible de percevoir immédiatement une conception centrale de ce discours.

Cela fait écho aux difficultés de la structuration du langage scientifique identifiées par Jean-Claude Passeron dans son ouvrage *Le Raisonnement sociologique*²²⁷. L'ensemble de l'ouvrage forme une anthologie de textes déjà publiés. Il s'intéresse sur le plan épistémologique à la pertinence descriptive des concepts typologiques utilisés en sociologie renvoyant notamment aux philosophies de Ludwig Wittgenstein, de Karl Popper, de Rudolf

²²⁴ Ces objets de référence s'articulent comme menacés à travers trois formes distinctes de sécurisation : l'hypersécurisation, les pratiques de sécurité de tous les jours et les technifications. HANSEN Lene, et NISSENBAUM Helen. « Digital Disaster, Cyber Security, and the Copenhagen School. » *International Studies Quarterly*, vol. 53, no. 4, 2009, pp. 1155–1175. Voir en particulier le chapitre 4.

²²⁵ Employé dans un usage analogue à celui de la sociologie législative, PERRIN Jean-François, « Jean Carbonnier et la sociologie législative », *L'Année sociologique*, Vol. 57, 2007, pp. 403-415.

²²⁶ Chez Jérémie Cornut, les excuses dans la diplomatie américaine. Cf. supra.

²²⁷ PASSERON Jean-Claude, *Le Raisonnement sociologique, l'espace non-poppérien du raisonnement naturel*, coll. Essais & recherches, Nathan, 1991, 408 p. L'ouvrage a connu des éditions revues et augmentées sous le titre *Le Raisonnement sociologique : Un espace non poppérien de l'argumentation*, sorti en 2006 et en 2013 chez Albin Michel qui n'a pas été employé dans cette recherche.

Carnap et de Max Weber... Nous nous concentrerons ici sur les premiers développements de l'ouvrage tiré de la thèse d'État de l'auteur en sociologie²²⁸.

Le monde conceptualisé par Passeron est tout ce qui « advient » reprenant la philosophie de Wittgenstein des faits dans l'espace logique qui constituent le monde²²⁹. Ce monde lorsqu'il est doté d'un caractère observable entre dans le domaine « empirique ». Le monde est dit « historique » lorsque le monde empirique observable ne peut se départir d'une référence spatio-temporelle. Cette référence est constitutive du monde historique. Une connaissance empirique du monde s'inscrit donc dans un rapport de vérité fondé sur l'observation de celui-ci. Cette connaissance est constituée d'assertions qui proposent une description articulée au sein d'un contexte (soit la partie concernée du monde historique). L'activité de recherche est donc formalisable en une proposition d'assertions. Une connaissance ne peut pas être purement descriptive car elle intègre toujours une forme de contextualisation²³⁰. L'ensemble des contraintes empiriques et historiques qui viennent juger la validité d'une proposition sont formalisées dans l'espace logique. Cet espace logique intègre l'ensemble des contraintes dans un sens de détermination de la « fausseté » et de la « vérité » ou de compatibilité et d'incompatibilité avec d'autres propositions. Cet espace logique se définit dans le référentiel de l'assertion dont la visée peut être le monde « possible », le monde empirique ou le monde historique. Pour définir le sens « assertorique » des propositions, il faut intégrer à l'espace logique l'ensemble des champs sémantiques des concepts qui forment « l'espace sémantique ».

1 – Nature du langage et conversation scientifique : le rejet épistémique de la forme logique de la réfutation.

Parce qu'elle entretient un lien de dépendance ou de contenance avec le sens de la proposition, cette composante de l'espace logique doit être regardée comme constitutive de celle-ci. Autrement dit, pour comprendre des concepts descriptifs du monde empirique, il est

²²⁸ Ibid. pp 31 à 56.

²²⁹ Bien que l'œuvre de Passeron commente notamment les travaux de Karl Popper, ce concept de monde est à distinguer de la métaphysique des trois mondes (Monde 1, Monde 2, Monde 3) que Karl Popper rapporte respectivement aux mondes des phénomènes physico-chimiques, du phénomène de conscience et des productions de l'esprit humain.

²³⁰ Ces éléments de contextualisation sont nommés « déictiques » par analogie avec les sciences linguistiques.

nécessaire d'interroger la relation qu'ils entretiennent non-seulement entre eux, mais avec des descriptions empiriques qui n'appartiennent pas forcément à un même univers de discours. Les sciences sociales sont un savoir empirico-rationnel à l'image des sciences de la nature mais d'une essence différente. Il y a ainsi une relation entre des concepts et une relation de ces concepts à l'empirie. Toute reformulation du sens d'une relation entre des concepts qui doit interroger leur relation au monde passe par cette démarche d'interprétation²³¹. La question posée est triple en ce qu'elle interroge la nature du « vrai » du monde empirique pour comprendre des faits du monde historique, la caractéristique probante du raisonnement sociologique dans la production de connaissance, et enfin les conditions empiriques d'une telle production scientifique tournée vers le monde historique.

L'épistémologie mise en place par Passeron se caractérise ainsi par trois propositions majeures. Tout d'abord, constitutive de nombreux langages de description du monde, la production de connaissance empirique doit résister à l'épreuve empirique rendue possible et nécessaire par la structure de ces mêmes langages. Or, il n'existe pas de langage unifié de la description empirique du monde historique. L'auteur ajoute qu'un tel langage est impossible²³². Enfin, la mise à l'épreuve empirique d'une proposition théorique qui cherche à comprendre le monde historique ne peut jamais revêtir la forme de la réfutation. En ce sens, la sociologie de Passeron s'affirme comme travaillant sur un espace « non poppérien ».

De la nature langagière non-uniforme de la connaissance scientifique, plusieurs conséquences sont à noter²³³ : la connaissance scientifique se place « hors et dans les murs de la cité scientifique ». La compatibilité de l'énoncé d'une proposition avec le réel se définit dans un espace sémantique. Seule la compatibilité d'un énoncé avec un autre se définit dans l'ensemble de l'espace logique. Ce dernier ne peut se comprendre comme porteur d'une expression de la réalité qui disqualifierait tous les autres énoncés qualifiant une même réalité. La mise à l'épreuve empirique est un critère d'évaluation des propositions qui fonctionne dans une science empirique laquelle suppose un accord de langage entre énoncé et réalité. Cet

²³¹ En cela, l'approche de Jean-Claude Passeron se rapproche davantage de l'épistème de Foucault que du paradigme de Kuhn pour le savoir en ce qu'il propose une vision de la connaissance scientifique animée d'une composante sémantique qui n'est pas uniquement confiné à « la science », mais à un large éventail de discours ancré dans sa propre époque.

²³² Ibid p.363.

²³³ Voir les conclusions de l'ouvrage pp 357 – 403.

accord peut se trouver dans un haut degré de consensus réalisé dans un groupe de spécialistes et exprimant un haut degré de stabilisation d'un langage de description du monde²³⁴.

Plus un langage scientifique bénéficie de normes et d'un haut degré de consensus, plus l'épreuve empirique qu'il suppose est déterminante pour la production connaissance dans le cadre d'une description définie²³⁵. Celle-ci est impossible en sciences sociales. Elles n'ont pas pour principe la production d'un savoir cumulatif. Leurs vulnérabilités et leurs pertinences empiriques ne peuvent être caractérisées que dans l'observation du monde historique et non dans l'expérimentation. Toute généralisation en dehors du contexte n'est possible que par un recours à une typologie présomptive distincte sur le plan méthodologique de l'idée de nécessité. L'équivalence, ou parenté, des contextes d'analyse hétérogènes par nature n'exclut pas chez le chercheur ce recours à la typologie. Cette observation ne peut s'épuiser dans une liste finie de propositions qui énonceraient les traits pertinents du contexte pour servir sa validité. L'analyse des variations et/ou covariations historiques à l'aune des variables permet de tenir un raisonnement formellement empirique.

Cette analyse demeure pourtant tributaire de l'interprétation en fonction du contexte de l'observation par le chercheur. Les concepts de cette analyse formalisés par le langage de la description du monde sont comparables en termes de statut dans l'espace logique aux définitions opératoires des sciences formelles ou expérimentales. Le plus souvent, ces concepts ne trouvent à se dire que dans un langage « naturel » car la forme des langages artificiels (une page d'équation) est impropre à les saisir totalement²³⁶.

L'universalité de telles analyses ne peut être qu'une universalité « numérique » délimitée par l'observation et pas « logique » applicable en tout temps et lieu (les seuls pouvant s'inscrire dans une logique de réfutation popperienne). Avec suffisamment de temps et d'énergie pour les énoncer, l'universalité numérique peut se comprendre comme une

²³⁴ L'auteur fait ici référence au concept de « paradigme » sur lequel nous sommes déjà revenus.

²³⁵ « La vulnérabilité et, donc, la pertinence empirique des énoncés sociologiques ne peuvent être définies que dans une situation de prélèvement de l'information sur le monde qui est celle de l'observation historique, jamais celle de l'expérimentation. »

²³⁶ Il ne peut être que momentané et instrumental. Pour « énoncer sur le monde historique » une assertion doit rester « solidaire de la sémantique des raisonnements qui lui ont permis d'immobiliser le sens des concepts et de ses relations. Le « recours à une langue artificielle, utile, précieux ou indispensable selon les cas » doit toujours être « retraduit après usage ». Ces énoncés ont « nécessairement plus de sens ». Voir Scolies Ibid pp.373 – 375.

addition d'énoncés singuliers contrairement aux seconds qui ne peuvent faire l'objet de ce remplacement. Par cette particularité, le concept se présente comme « un intermédiaire entre le nom commun et le nom propre »²³⁷, à mi-chemin entre empirie et théorie.

2 – Espace sémantique, occurrences et évènements.

Du point de vue de la connaissance, les sciences sociales ont donc un statut mixte auquel elles ne peuvent accéder que par la maîtrise de l'espace sémantique. Cette maîtrise passe par une structure nécessairement typologique et exclut la définition stricte des conditions initiales d'une observation. Une science humaine si elle cherche à s'inscrire dans le modèle des sciences expérimentales se retrouve placée dans le dilemme popperien (empirie contre métaphysique) qui ne laisse le choix qu'entre l'exemplification²³⁸ et la falsification comme seule épreuve pour définir sa pertinence empirique. Dans sa lecture de Karl Popper et de Gaston Bachelard, Passeron applique une grille de lecture qui distingue l'occurrence et l'évènement. Si l'occurrence est la survenance d'un fait, il faut que celle-ci soit répétée pour créer un effet reproductible qui réfute une théorie²³⁹. Telle occurrence est donc une décomposition d'un événement mu par un contexte particulier.

Cela amène l'auteur à qualifier les sciences expérimentales de sciences de l'événement et les sciences historiques (au nombre desquelles les sciences sociales) de sciences de la co-occurrence. La réfutabilité d'une théorie constitue un modèle de preuve d'une vulnérabilité empire optimale. La corroboration d'une théorie réside ainsi dans le fait qu'elle continue à passer des tests falsificateurs. Si Passeron reconnaît à cette forme, la « logique » de la découverte scientifique à défaut de son « histoire » ou de sa dimension « psychologique », il lui reproche son manque de distance par son adhésion solidaire au modèle de pertinence des sciences « physico-expérimentales ».

Sur la casuistique qu'implique l'exemplification, la présence d'une méthode ne réduit pas leur vulnérabilité empirique et donc préserve une forme de valeur démonstrative envisagée

²³⁷ Ibid. p.379. L'auteur prend l'exemple du sens du « féodalisme » qui ne peut être qu'imparfaitement traduit par la seule énumération des propriétés économiques, juridiques, mentales, militaires... auprès d'une personne qui ignoreraient tout de l'Occident médiéval, du Japon de l'ère Kamakura ou de la Chine des Royaumes Combattants...

²³⁸ L'exemplification ou constat érigé en exemple, ne doit pas se limiter à des constats empiriques à valeur probatoire nulle.

²³⁹ Ibid. p. 387.

de manière différente à la logique de la réfutabilité. Cette valeur devrait être décrite pour chaque raisonnement sociologique. Cela passe par une reconnaissance du fait que les sciences sociales ne peuvent complètement s'extraire du raisonnement naturel. Malgré les détours permis par les techniques, la chaîne argumentative qui supporte la force de l'assertion est aussi faible que son maillon le plus faible : l'espace sémantique. C'est la raison pour laquelle les démarches de tout raisonnement descriptif ou comparatif tenu par quelque langue scientifique que ce soit pour peu qu'il cherche à s'appliquer au monde historique entre dans les présentes considérations épistémologiques.

Dans cet espace sémantique où se trouve la pertinence ? Elle croît dans les exigences d'une grille conceptuelle de description du monde historique dans l'exemplification formée des contraintes empiriquement multipliée et sémantiquement conjointes. Les seuls ressorts possibles de l'épreuve empirique pour les sciences sociales résident dans l'organisation des constats empiriques par une sémantique protocolisée. Les dispositifs expérimentaux doivent demeurer accessoires, autonomisées du raisonnement premier. Ils sont donc neutralisés de l'évaluation de la pertinence assertorique du raisonnement tenu. Les questions relatives au monde historique existent cependant dans toutes les sciences de la matière et la vie. L'ouvrage évoque ici une relation à la question de la causalité en expliquant qu'il est plus facile d'interroger les faits « de la nature » (l'origine de la vie) que les faits « humains » (les causes d'une guerre).

Cette différence procède de l'existence d'un savoir nomologique constitué ou en voie de constitution qui n'existe pas en sciences sociales. Ce faisant le naturalisme qui préside l'espoir de la naissance d'une science « nomologique-mère » comme le furent « l'économie, la démographie, la psychologie ou la linguistique » ne peut conduire qu'à la « déception ». En cela, l'auteur revient sur les positions épistémologiques en sociologie des sciences de Robert King Merton qu'il qualifie d'« illusion de Merton » et taxe de type messianique. Pour l'auteur, le « nombre de prétendants au rôle de messie théorique [...] ne font des miracles qu'aux yeux de la secte »²⁴⁰. L'illusion nomologique par l'inadéquation qu'elle suppose par une argumentation inadéquate ne produit pas seulement des « connaissances illusoires » mais

²⁴⁰ Ibid. p. 388. Sur ce que l'auteur qualifie comme illusion de Merton voir la scolie consacrée pp. 365 – 366.

déplace ou affaiblit tout à la fois le sens des connaissances produites et la finalité de son système de production de connaissances²⁴¹.

3 – Concepts polymorphes et sténographiques face à la circulation des idées dans l'espace sémantique.

Pour confronter le statut logique du lexique des sciences sociales et dégager l'importance de la sémantique, il suffit « de soumettre ces mots à une épreuve » toute discipline confondue²⁴². Ces notions n'apparaîtront pas en sciences sociales comme liées à des opérations formelles organisant une observation généralisable par induction ou un « protocole-type » qui épouserait la connaissance utile des conditions de l'observation à peine d'artifice.

Deux obstacles viennent rendre cette tâche un peu vaine. D'une part, le passé opératoire d'un concept constitue sa dimension sémantique. Plus il possède une portée générale, plus le concept sera détaché des effets de connaissance qu'il a effectivement produit. D'autre part, le concept s'il est trop ancré dans le monde réel, sur un état de fait qu'il décrit, et n'est que peu articulé avec la théorie.

En un mot, les concepts sont soit trop théoriques, soit trop peu théoriques. La typologie se construit donc dans une abstraction qui juxtapose « le trop » et « le trop peu ». Par trop théorique, Passeron entend que le concept a une histoire marquée par la multiplicité des emplois descriptifs : il s'agit du concept polymorphe. Il qualifie de ce type de concept de « résidu scolaire » inopérants, concentrés, sans vigueur, ni indexation, qui ne trouve sa seule force que virtuellement *a posteriori* dans le résultat de la recherche qu'il a permis au chercheur de construire²⁴³. Un concept polymorphe se rencontre lorsque le chercheur fait face à cette multiplicité de sens et que celle-ci ne peut être maintenu virtuellement derrière son emploi.

Quand le concept est trop peu théorique, le chercheur fait face à un concept sténographique qui se matérialise linguistique dans des variations de formes.*ad hoc* qui ne trouve leur sens que dans un contexte et des relations aux faits spécifiques. Lorsque l'on

²⁴¹ Ibid. p. 393.

²⁴² Ibid. p. 36

²⁴³ Ibid. pp 37 - 39

s'intéresse au langage du cyberspace, la distinction entre un concept trop théorisé ou trop peu ne fait plus réellement sens. En tant que mot-valise susceptible de beaucoup d'approches différentes et de déformations, le cyberspace voit son étude déformée par la circulation des idées et la circulation internationale des idées²⁴⁴.

Cet usage du cyberspace dans le langage se traduit de trois manières : soit il produit un terme dérivé issu de l'adjonction d'un préfixe « cyber- » à n'importe quel mot qui semble idoine à la personne qui l'emploie, soit il appelle différentes définitions qui viennent modifier le sens des premières variations. Un dernier usage est celui d'invoquer « le » ou « la » cyber, comme un substantif animé d'un sens propre sous-entendu dans l'utilisation. Il y a donc une prolifération qui dépasse le simple nombre pour opérer des variations de formes et de sens dans un ensemble discursif non-figé doté d'une croissance rapide.

Nous aurions donc à traiter d'un phénomène inobservable que nous serions incapables de traduire sous la forme de concept. Laquelle conceptualisation nous est pourtant nécessaire afin d'opérer la traduction du phénomène en question permettant la combinaison que nous souhaitons opérer.

²⁴⁴ La circulation internationale des idées a notamment fait l'objet d'un numéro des *Actes de la recherche en sciences sociales* avec une introduction mobilisant une conférence donnée par Pierre Bourdieu en 1989 à l'université de Fribourg où il évoque plusieurs facteurs créateurs de malentendus internationaux dans les échanges scientifiques : les textes circulent sans les contextes par lesquels ils sont déterminés (champ de production), . BOURDIEU Pierre. « Les conditions sociales de la circulation internationale des idées ». In: *Actes de la recherche en sciences sociales*. Vol. 145, « La circulation internationale des idées », décembre 2002. pp. 3-8.

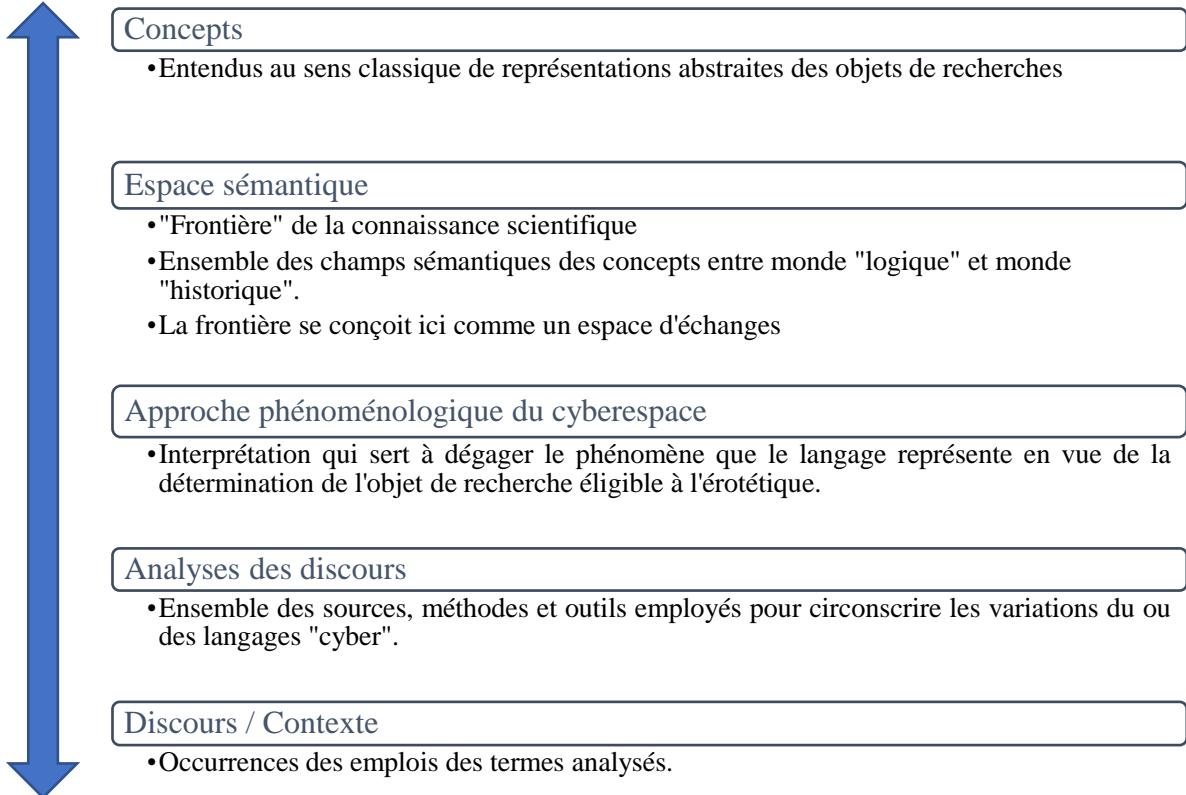


Figure 2 – Résumé de la conceptualisation de l'objet par une approche discursive.

4 – Epistémologie de Jean-Claude Passeron et Relations Internationales.

Ayant esquissé les contours de la sociologie de Jean-Claude Passeron, se pose la question de sa compatibilité avec les Relations Internationales. De façon générale, la sociologie questionne la construction des Relations Internationales à travers les concepts, des postures de recherches et des cadres méthodologiques qu'elle offre à travers ses nombreuses approches²⁴⁵. Ainsi, elle peut s'inscrire dans les débats des théories des Relations Internationales en offrant les objets et les outils d'une épistémologie réflexive²⁴⁶. De l'approche de Jean-Claude Passeron, nous retiendrons avant tout une forme de sociologie de

²⁴⁵ RAMEL Frédéric, « Chapitre 22. La sociologie », In. BALZACQ Thierry et RAMEL Frédéric (dir), 2013, op-cit, pp. 499-522.

²⁴⁶ MERAND Frédéric et POUILLOT Vincent, « Le monde de Pierre Bourdieu : Éléments pour une théorie sociale des Relations internationales », *Revue canadienne de science politique*, vol. 41 n°3, 2008, pp. 603 – 625. *

la connaissance qui veut que toute production à caractère scientifique soit issue d'un contexte particulier et peut être comprise sous l'angle de la pratique²⁴⁷.

L'apport de la sociologie de Jean-Claude Passeron est triple. Au plan épistémologique, premièrement, elle favorise une compréhension de la connaissance scientifique par le biais du contexte. Deuxièmement, la conséquence principale du recours à cette sociologie implique une ouverture à la fois sur la différence et les influences réciproques des discours scientifique et politique et sur la spécificité des phénomènes internationaux dans l'ensemble des phénomènes sociaux. Elle implique un rejet de l'assertion qui conviendrait que la différence d'échelle emporte une différence de nature des phénomènes politiques. Troisièmement, l'approche sociologique vient faciliter à la fois la définition de l'objet ainsi que le croisement des méthodes et des théories différentes. Cet apport formera le socle de l'étude de discours qui permettra d'accueillir chacun des volets de notre approche phénoménologique plurielle du « cyberspace » et sa compatibilité avec la combinaison pragmatique.

Section 3 – Dépasser le nominalisme : Etude de discours et approche phénoménologique plurielle du « cyberspace ».

En tant qu'objet sémantique, le cyberspace a conduit à identifier plusieurs niveaux de phénomène qu'il faut déconstruire : les dimensions lexicale, discursive et idéelle. En tant que phénomène du langage, le cyberspace s'entend d'abord d'une variation de substantifs (lexiques), d'une utilisation particulière (discours) elle-même porteuse de sens (systèmes de sens). C'est ce contexte qui fonde le phénomène et qui légitimise son insertion dans les Relations Internationales et plus largement dans la Science Politique. La volonté de trouver une définition serait vouée à l'échec. Etant un objet discursif, l'expression ne doit pas être considérée en elle-même dans une logique de définition, mais dans une logique d'explicitation ou de compréhension. Aux questions de savoir ce que signifie le cyberspace et que signifient ses variations, il faut comprendre comment il est utilisé. Cette approche visant à traduire le cyberspace dans un phénomène observable pour les Relations Internationales aura un caractère plural. Cette étude du discours fera l'objet de la première partie de ce manuscrit. A

²⁴⁷ Déjà présente, lors de ses travaux avec Pierre Bourdieu et Jean-Claude Chamboredon. BOURDIEU Pierre, CHAMBOREDON Jean-Claude, PASSERON Jean-Claude, *Le Métier de Sociologue*, Paris, École Pratique des Hautes Études, Mouton and Bordas, 1968, 432 p.

chacune des étapes de l'étude correspondent des conceptions méthodologiques particulières qui constituent en elles-mêmes les applications de la stratégie de recherche.

Les conclusions tirées de cette approche phénoménologique formeront la première partie du manuscrit. Se pose tout d'abord la question de l'origine du phénomène et de son impact sur le langage. Cette question de l'origine sera confrontée aux diverses influences culturelles et scientifiques afin de déconstruire le mythe de l'invention de ce terme et voir comment les idées qui en découlent sont un élément qui forme une influence de son utilisation. Dans un second temps, il nous faudra confronter l'impact du phénomène dans la production normative à un niveau régional, européen et onusien. Enfin, il faudra revenir sur les appropriations particulières de ce langage dans une forme de conceptualisation. Cette dernière analyse s'effectuera à travers l'observation d'une institutionnalisation d'une communauté discursive en France revendiquant une forme d'appropriation dudit langage.

A – Des récits à l'histoire des idées : éléments pour une généalogie du cyberespace.

Dans l'ouvrage tiré de ses travaux de thèse, Benjamin Loveluck évoque l'idée d'une généalogie politique d'Internet²⁴⁸. Si Internet est compris dans l'objet d'étude formé du cyberespace et ses variations, ce dernier ne s'y résume pas. Il en va de même pour la plupart des objets techniques qui y sont associés. La solution adoptée consiste à se concentrer sur le lexique et la prolifération dont il est l'objet à partir d'un point de départ : son invention dans la littérature. Le cyberespace s'envisage comme un produit littéraire assemblé dans un contexte particulier avec ses contraintes de production mais aussi un héritage culturel et scientifique. À travers ce rapport de forces qui préside à la production du terme « cyberespace » puis de son succès, se trouve l'idée qu'il véhicule. Cette idée est plus large que la sécurité de l'information et permet d'éviter l'épineuse question de la définition technique de l'objet. C'est la réception puis la réappropriation du terme qui créent la prolifération. La mise en avant des contraintes pesant à la fois sur sa production, sa réception et sa réappropriation, permet de circonscrire le référent de l'analyse et de commencer à analyser la prolifération. Le moment clef pour débuter l'analyse n'est donc plus cette « cyberguerre venue du froid » depuis les événements politiques de 2007, mais la littérature

²⁴⁸ LOVELUCK Benjamin, *Réseaux, libertés et contrôle : Une généalogie politique d'internet*, Paris, Armand Colin, 21 oct. 2015, 368 p. Ouvrage tiré d'une thèse, *La liberté par l'information : généalogie politique du libéralisme informationnel et des formes de l'auto-organisation sur internet*, thèse soutenue en 2012 à l'EHESS, Paris I, sous la direction de Marcel Gauchet.

de science-fiction à partir de 1982. Il s'agit donc ici d'un premier pas dans la déconstruction du récit que nous évoquions en début de manuscrit. De plus, cette approche ne s'intéressera pas au cyberespace pour lui-même qu'au pouvoir évocateur du terme. Ce qui permet de déconstruire deux autres types de récits partiels que sont ceux fondés sur une acceptation « contre-culturaliste » et les visions « écosystémique » sociales-libérales ou conservatrices.

Ce rejet de la définition technique du cyberespace tient compte du caractère inépuisable du réel qui fonde la situation d'anarchie des concepts dans l'espace sémantique et la liberté dans leur découpage. Parce qu'il est d'essence littéraire, le terme cyberespace ne possède en effet qu'un sens construit. Ce sens est d'abord limité au cadre de l'œuvre de l'esprit qui l'a vu naître, mais également dans sa réception. Au-delà du contenu de l'œuvre de l'esprit, les contraintes liées à la production s'inscrivent dans une double-dimension téléologique et historique. D'une part, l'invention du cyberespace était conditionnée par un ensemble de finalités propres à l'auteur. D'autre part, l'invention du cyberespace est le produit de l'association ou la contraction de termes déjà existants dans une configuration qui n'était pas inédite à l'époque (le « cyborg » et la « guerre cybernétique » notamment).

Enfin, les récits sont des structures narratives prescriptives et prédictives qui illustrent une forme de relation causale entre les faits sociaux instituée par une dimension dramatique et non-démonstrative. En ce qu'il interroge la production, la diffusion et l'adhésion de la connaissance, le récit est un objet de compréhension de l'ordre social et fonde la dimension critique de cette recherche. Au-delà des idées, l'analyse du récit est une forme d'étude privilégiée dans les approches critiques des politiques publiques²⁴⁹ mais également dans l'étude de la construction des identités collectives. A titre d'exemple, la question des minorités fait l'objet d'un certain nombre d'étude où l'étude des récits et l'analyse de discours jouent un rôle prépondérant. Ces deux approches permettent d'identifier des articulations discursives particulières entre l'État et les individus qui sont en compétitions avec différentes stratégies

²⁴⁹ ROE Emery, *Narrative Policy Analysis: Theory and Practice*, Duke University Press, 1994, 199 p. Parmi les études les plus célèbres, on peut notamment citer l'étude de Claudio Radaelli sur le récit de la « concurrence fiscale nuisible » entre les États de l'Union Européenne. RADAELLI, Claudio M., « Harmful Tax Competition in the EU: Policy Narratives and Advocacy Coalition », *Journal of Common Market Studies*, 37, 1999, pp 661-682. Voir également RADAELLI Claudio M. « Logiques de pouvoir et récits dans les politiques publiques de l'Union européenne », *Revue française de science politique*, n°2, 2000. pp. 255-275

d'unification et de différenciation²⁵⁰. Le pouvoir évocateur du cyberespace s'oppose paradoxalement à un autre principe qui est celui de l'évacuation de l'idéal. Les expressions du cyberespace opèrent dans une forme de nouvelle matérialité fondée sur une *praxis* numérique qu'elle soit d'inspiration économique, technique, ou juridique. Les éléments de discours cherchant à promouvoir la sécurité des États ou des libertés individuelles sont finalement peu favorables à la production d'idées. Les tentatives de coopération sont quant à elle un moyen rationnel de protection, par le partage des coûts et des ressources.

Compris en négatif, le « pouvoir évocateur » forme le medium permettant la circulation de la notion de cyberespace entre les mondes littéraires, scientifiques, économiques et politiques ainsi que ses variations. Ce n'est que parce que la notion fait l'objet d'appropriation et de différentes conceptualisations que l'on peut le découvrir. Autrement dit, le pouvoir évocateur se comprend négativement. Dans le cadre de cette recherche, il est une composante intersubjective de la signification qui recouvre l'ensemble effectif du contenu symbolique du terme. Il ne s'agit pas de donner au cyberespace une signification nouvelle mais de dégager les ensembles de significations (ou systèmes de sens) qui sont eux-mêmes révélateurs des phénomènes sociaux que nous tentons d'approcher par cette étude.

B – Impact normatif du cyberespace et des termes dérivés : bases de données, observation statistique et analyse logométrique.

Comme d'autres ensembles théoriques les définitions opératoires tirées de l'analyse de discours ne font pas consensus. Il serait ainsi important de distinguer au sein de l'analyse du discours, les analyses de contenus. L'analyse de discours est une posture théorique et une méthode d'analyse qui vise l'étude du sens latent d'un texte et peut s'exercer de manière qualitative ou quantitative, compréhensive ou critique. L'analyse de contenu est une méthode qui vise à dégager le sens manifeste d'un texte au profit de tout type d'approche théorique mais avec des outils principalement quantitatifs.

La lexicométrie consiste pour sa part à objectiver le texte par l'étude des occurrences de divers mots (lexique)²⁵¹. La logométrie, s'inscrit dans le prolongement de cette tendance

²⁵⁰ WEINBLUM Sharon et DANERO IGLESIAS, Julien, « The discursive exclusion of minorities: A study of identity discourse in Israel and Moldova », *Critical Approaches to Discourse Analysis across Disciplines Journal*, 7(1), 2013, pp. 164-179

²⁵¹ BAILLAT Alice, EMPRIN Fabien, RAMEL Frédéric, op-cit.

en combinant une lecture qualitative et une lecture quantitative de corpus à la fois dans les unités du discours et dans sa globalité. Elle dépasse donc la simple mesure du lexique. L'ensemble des opérations de recherche dites de logométrie a été effectué avec le logiciel libre IRaMuTeQ (Interface de R pour les Analyses Multidimensionnelles de Textes et de Questionnaires)²⁵² ²⁵³. Le choix s'est porté sur ce logiciel à l'issu d'une période de recherche et d'essais sur différents logiciels (Lexico 2 et 3, Hyperbase...).

L'introduction de l'outil informatique semble à première vue plutôt neutre au regard de son apport à la question ontologique du discours. En effet, l'outil informatique pour l'analyse de discours consiste essentiellement dans une contrainte formelle supplémentaire : c'est d'abord un outil au service d'une méthode. Néanmoins, il invite le chercheur à expliciter ses procédures de lecture. L'informatique oblige l'analyse de discours à partir de la forme du texte. Cette forme pourra être comprise à travers différents niveaux de complexité. Ce n'est donc pas tant les capacités de calcul d'une machine qui posent question que l'impact induit par la formalisation de ces niveaux de complexité. De là, procède un second apport, critique, de l'outil informatique dans la remise en cause de l'objectivisation du discours conduite par le chercheur. En cela, l'outil informatique ne peut pas résoudre des problèmes théoriques que les autres sciences ne peuvent trancher. Il ne substitue pas à l'analyse²⁵⁴. A ce titre, cette étude sera également nourrie par les résultats des différentes enquêtes menées au cours de cette recherche.

La logométrie est-elle compatible avec les Relations Internationales ? Comme le soulignent Frédéric Ramel, Alice Baillat et Fabien Emprin, l'utilisation d'outils statistiques s'appliquant aux mots du discours, est peu investie pour l'étude des Relations Internationales. Même s'ils permettent de disposer d'outils « utilisables pour dépasser ces difficultés et révéler au chercheur des aspects non détectables manuellement » ²⁵⁵. Ils ajoutent : « Comme tout traitement quantitatif, l'utilisation de la lexicométrie suppose des précautions. Le traitement

²⁵² Interface logicielle fonctionnant sur la base du langage R sous licence GNU GPL.

²⁵³ Pour une autre étude réalisée avec plusieurs outils de logométrie et qui permet de mesurer la plus-value d'IRaMuTeQ sur des études de même type : voir GUARESI Magali, « Les thèmes dans le discours électoral de candidature à la députation sous la Cinquième République. Perspective de genre (1958-2007) » In. BEN HAMED Mahé et MAYAFFRE Damon (dir.) « Thèmes et thématiques dans le discours politique », *Mots, Les langages du politique*, n°108, 2015, 180 p.

²⁵⁴ DUCHASTEL Jean, Ibid. p. 1631.

²⁵⁵ BAILLAT Alice, EMPRIN Fabien, RAMEL Frédéric, op-cit, §2-17

informatique aura des difficultés à tenir compte de la polysémie des termes et des homonymies »²⁵⁶. C'est un risque minime concernant notre objet d'analyse. D'autres auteurs soulignent la possibilité d'étudier de large ensemble de données²⁵⁷.

Chez Jean-Claude Passeron, l'énonciation statistique « devient *ipso facto* énonciation sociologique » à partir du moment où elle porte sur le monde historique car l'assertion sociologique emporte sa propre désignation sur les éléments statistiques qu'elle mobilise²⁵⁸. La question de l'apport de la statistique à la démarche de la combinaison semble plus délicate. Jérémie Cornut établit une distinction assez nette entre l'approche quantitative et l'approche qualitative (étude de cas)²⁵⁹. Son objet d'analyse (les excuses dans la diplomatie américaine) est un phénomène « trop complexe pour pouvoir être modélisé ou réduit à un petit nombre de variables susceptibles d'un traitement informatique ou mathématique et ses occurrences sont relativement limitées » (46)²⁶⁰.

1 – Outils conceptuels pour l'emploi d'une approche logométrique.

Le concept clef de l'analyse de discours est le corpus. Celui-ci est envisagé comme la construction finalisée d'un dispositif d'observation empirique à partir de données textuelles²⁶¹. Loin d'être dispensable, la construction du corpus est essentielle dans la mesure où elle répond à la question de savoir pourquoi un texte est lu et constitue une condition de l'interprétation. Dans le cadre de notre étude de variation, nous nous intéresserons à deux types de données : l'occurrence et la cooccurrence. Si l'occurrence se comprend aisément comme la présence d'un mot dans le corpus, la cooccurrence mérite un peu plus d'attention.

Héritière de la linguistique anglosaxonne, une cooccurrence se comprend comme une présence simultanée de deux mots dans le même énoncé (contexte). Le concept de

²⁵⁶ Ibid, §9

²⁵⁷ MANSFIELD, Edward D. et PEVEHOUSE Jon. « Democratization and the Varieties of international Organizations. », *Journal of Conflict Resolution*, 52(2), 2008, pp. 269-294.

²⁵⁸ PASSERON, op-cit, pp 204 - 205.

²⁵⁹ CORNUT, op-cit, pp 203 - 205.

²⁶⁰ Ibid, p. 205.

²⁶¹ En ce sens : CHARAUDEAU Patrick et MAINGUENEAU Dominique, *Dictionnaire d'analyse du discours*, Paris, Le Seuil, 2002, 661 p. ainsi que MAYAFFRE Damon, « Introduction » In. « Les corpus politiques : objet, méthode et contenu », *Corpus*, 4, 2005.

cooccurrence est en sciences linguistique le fondement du champ lexical ou de la thématique (isotopie)²⁶². En cela, la cooccurrence apparaît dans la plupart des études, des méthodes et des outils logométriques comme un outil privilégié des approches thématiques. A l'échelle du corpus, cette cooccurrence désigne la présence de deux substantifs dans une même subdivision du corpus²⁶³.

Cette recherche retient ainsi une acceptation différentielle de la cooccurrence qui s'appuie sur une unité contexte qui dépasse le seul cadre de la phrase. La cooccurrence est donc un fait observable à la fois statistique et textuel : elle incarne l'unité minimale formalisable d'une relation entre deux mots (et donc du contexte d'un mot par un autre²⁶⁴). La cooccurrence est un objet qui permet de tenir compte de la matérialité discursive d'un corpus à la fois de manière quantitative et qualitative, décontextualisée et recontextualisée²⁶⁵. La limite majeure de la cooccurrence est son côté descriptif. En effet, si elle permet de fournir un résultat qui décrit l'état du corpus donné, elle ne fournit pas d'approche causale et ne dispense pas le chercheur de son travail d'interprétation.

Si une cooccurrence donnée ne vaut que pour elle-même, l'agrégation de l'ensemble des cooccurrences ne saurait se résumer à un simple inventaire au même titre que le recensement des seules occurrences. En effet, la cooccurrence ne peut se réduire à une « occurrence partagée » ou une « occurrence ensemble » car elle constitue un réseau²⁶⁶ et

²⁶² Cette recherche n'a pas vocation à rentrer dans la question de la nature plus spécifique des liens linguistiques de cooccurrence entre les termes qu'elles soient relatives au sens (synonymie, antonymie etc.) ou qu'elles soient formelles (syntagmes figés, expressions, collocations) ... Sur cette question et sur l'importance de la collocation dans le développement de cooccurrence, voir notamment le numéro collectif de la revue *corpus* : MAYAFFRE Damon et VIPREY Jean-Marie (dir.) « la cooccurrence : du fait statistique au fait textuel », *Corpus*, n°11, 2012, en particulier LEGALLOIS Dominique, « La colligation : autre nom de la collocation grammaticale ou autre logique de la relation mutuelle entre syntaxe et sémantique ? », *Corpus*, n°11, 2012, pp. 31 -54.

²⁶³ Cette subdivision au sein du corpus peut généralement être comprise de trois manières : soit, elle est opérée par le chercheur (différents textes par exemple), soit elle résulte de la prise en compte de la ponctuation (phrase, paragraphe...), soit elle est une mesure arithmétique (en nombres de signes ou en nombres de substantifs).

²⁶⁴ MAYAFFRE Damon, « De l'occurrence à l'isotopie. Les co-occurrences en lexicométrie », *Sémantique & Syntaxe*, n°9 p. 53 à 72, 2008.

²⁶⁵ L'objet permet également de tenir compte tout à la fois de la dimension syntagmatique et paradigmatische du discours, soit les structures de contiguïté et de similarité des substantifs en question.

²⁶⁶ MAYAFFRE Damon et VIPREY Jean-Marie, 2012, op-cit, p. 12 et 13.

permet de mettre en valeur la textualité du corpus²⁶⁷. C'est à partir de cette dernière idée que se développent la plupart des approches « métriques » en opérant une forme de restriction du modèle classique de la cooccurrence par l'adjonction d'un principe hiérarchique qui pourra permettre d'utiliser des cooccurrences complexes^{268 269}. Une première possibilité réside dans les « poly-occurrences ». Le principe revient à calculer les cooccurrences de manière répétées entre un premier et un second substantif, puis entre le premier et un suivant, afin de disposer des cooccurrences entre les trois substantifs. Le procédé est extensible et restitue les chaînes de cooccurrences. Une seconde possibilité existe avec les « trames de cooccurrences » qui reviennent à calculer les cooccurrences de chacun des substantifs à analyser.

« De fait, l'aspect circulaire de certaines grappes dans le réseau clarifie la hiérarchisation des nœuds en dégageant les formes à valence lexicale élevée qui sont plus importantes sur le plan de la structuration sémantique du texte. Peu nombreuses, ces formes occupent une position centrale sur le graphe tandis que d'autres, telles de nombreux satellites, viennent les compléter pour former des constellations lexicales sémantiquement homogènes. »²⁷⁰

Lors des calculs des cooccurrences, le corpus dans son ensemble ne peut être classé dans des mondes lexicaux. Cela suppose une perte d'information plus ou moins importante qu'il est nécessaire de contrôler. Cela implique un travail de reconstitution qui implique une bonne connaissance du corpus analysé en cohérence avec la posture retenue²⁷¹.

2 – Impact normatif et sélection des corpus.

Parler de l'impact normatif d'une notion, c'est se concentrer sur une forme particulière de réception de celle-ci : les normes qui découlent de son appropriation. De la cadre de

²⁶⁷ « Concept de “textualité”, défini comme la caractéristique d'un objet sensible appréhendé de façon spatiale et qui s'adresse à la compréhension d'un lecteur en jouant à la fois sur la mise en rapport systématique de propositions élémentaires placées en contiguïté et sur des rappels plus ou moins lointains, continus et réglés d'éléments présentés en amont. » VANDENDORPE Christian, *Du papyrus à l'hypertexte*, Boréal, Montréal, La découverte, Paris, 1999, p. 31

²⁶⁸ MARTINEZ William, « Au-delà de la cooccurrence binaire... Poly-cooccurrences et trames de cooccurrence », Corpus, n°11, 2012, pp. 191 – 218.

²⁶⁹ Voir notamment les trois catégories suivantes : « les cooccurrences spécifiques révèlent des attractions binaires, les poly-cooccurrences extraient des systèmes cooccurrentiels avérés en contexte, enfin les trames dévoilent la totalité cooccurrentielle du texte. », Ibid, p. 214.

²⁷⁰ MARTINEZ William, op-cit. p. 210.

²⁷¹ CHARAUDEAU Patrick, « Le chercheur et l'engagement. Une affaire de contrat », *Argumentation et Analyse du Discours*, 11, octobre 2013.

l'analyse logométrique nous nous focaliseront d'une part sur une appropriation de la notion par des objets de référence classiques que sont l'État et les organisations internationales, puis plus généralement dans les médias.

Cette étude logométrique porte sur des textes avec une approche longitudinale (2001 – 2016) et dans une perspective multiniveau à partir du cas français. Si les diverses archives et bases de données à notre disposition nous permettait de remonter jusqu'aux débuts des années 90, en pratique l'absence de résultat probant dans le corpus institutionnel, nous a conduit à retenir l'étude lexicale de 2001 produite par Rachèle Raus comme point de départ²⁷² ²⁷³. Du point de vue de la forme, cela permettait de commencer les études à partir des premiers résultats observables. Du point de vue du fond, cet article nous fournir les sens les plus communs des expressions dérivées du cyberspace et nous permet de disposer d'une vision du thème du cyberspace²⁷⁴.

A partir de cette étude, la période d'étude a été fixée à une quinzaine d'années, plus précisément de février 2001 à octobre 2016, ce qui était le maximum exploitable dans le cadre du calendrier de la thèse. Les différents corpus d'étude sont donc construits autour des « champs » : institutionnels et médiatiques, au sein desquels nous mettrons en lumière les caractères majeurs liés aux usages du cyberspace en recourant à l'approche thématique. Le critère majeur de la construction de ces différents ensembles thématiques réside dans l'usage du terme cyberspace et de ses dérivées²⁷⁵.

Dans cette recherche, les cinq corpus²⁷⁶ ayant fait l'objet d'une analyse logométrique sont :

²⁷² RAUS Rachèle, « Productivité de cyber et hyper dans le lexique français d'Internet », op-cit. De plus, le 23 novembre 2001 a été mise à la signature la *Convention de Budapest* ou *Convention sur la cybercriminalité* dans le cadre du Conseil de l'Europe. 2001 semblait ainsi une très bonne année pour débuter l'analyse statistique.

²⁷³ Ce point premier point de départ a été enrichi à partir de l'ouvrage suivant : OTMAN Gabriel, *Les mots de la cybersulture*, Belin, 1998, 474 p.

²⁷⁴ Il s'agit des ensembles de signification décrits pour les dérivés du cyberspace en chapitre liminaire : la réalité virtuelle, la cybernétique comme branche de la robotique, ainsi que tout et n'importe quoi du moment que « cela se rapporte à l'Internet et aux réseaux multimédias interactifs du futur de l'an 2000 ». Ibid.

²⁷⁵ La règle générale était la suivante : « le corpus d'étude se compose de tout texte publié dans la période donnée utilisant le cyberspace ou un terme voisin, y compris les expressions « cybernétique », « cyber » et à l'exclusion du mot « cyborg ».

²⁷⁶ Un autre corpus dédié à la presse avait été prévu à l'origine sur la base de donnée Europresse, mais il n'a pu être réalisé par manque de temps.

1. L'ensemble des publications du journal officiel de la République française entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé.
2. L'ensemble des publications du journal officiel de l'Union Européenne entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé.
3. L'ensemble des publications du système de diffusion électronique des documents de l'ONU en français entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé.
4. L'ensemble des publications francophones de presse généraliste et spécialisée entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé disponibles sur la plateforme Factiva.
5. L'ensemble des publications francophones de presse généraliste et spécialisée entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé sur la base de données de Google News.

L'outil logométrique vise principalement à circonscrire une partie du phénomène qui constitue l'hypothèse de travail de cette recherche²⁷⁷. Le principe est de pouvoir définir l'appropriation de la notion horizontalement par ses variations dans le temps, et verticalement dans les différentes échelles d'appropriation (individus, collectivités territoriales, État, échelle régionale, échelle internationale). L'intérêt de ne retenir que le cas français dans cette analyse est la construction d'un point de référence de nature à permettre la démarche érotétique dans un second temps. Il s'agit également d'un critère de faisabilité de l'étude. Pour chaque corpus, l'ensemble des textes doit appartenir au même univers linguistique et culturel afin de permettre la comparaison. En effet, la comparaison logométrique sur la base de plusieurs langues suppose en effet un travail plus complexe que celui qui était permis dans le temps de cette recherche. S'il est possible de multiplier les corpus d'analyse en fonction de chaque État de référence. Chaque analyse ne vaudra que dans l'État en question car le corpus constitué sera différent d'un état à l'autre. Se pose également le problème de la traduction.

Le corolaire réside dans le fait qu'une telle démarche est fortement dépendante de la production normative du collectif émetteur. Si l'ensemble des documents n'est pas disponible

²⁷⁷ Le recours à cette approche est en partie liée aux contraintes inhérentes à l'objet. Cf. difficultés rencontrées (Section V).

dans la langue de travail idoine, il est impossible de constituer un corpus qui viennent s'intégrer à l'étude. C'est la raison pour laquelle des organisations n'ayant pas l'intégralité ou la quasi-intégralité de leur production disponible en français n'ont pas pu être intégrées à l'étude. C'est notamment le cas de l'OTAN.

3 – Optimisation de moteurs de recherche : développement de l'agent logiciel GnOSIE.

Cette recherche a été l'occasion de travailler sur un agent logiciel expérimental en javascript afin de disposer d'un outil léger, gratuit et *open source* qui permette de collecter, rassembler et de mettre en forme une vaste quantité de documents afin de former des corpus d'étude pour le logiciel IRaMuTeQ, à partir de Google News²⁷⁸. Ce bot informatique appartient à la famille des techniques d'optimisation pour les moteurs de recherche, ou SEO (*Search Engine Optimization*). Cet outil a vocation d'une part à réduire le temps de collecte des nombreux résultats d'un moteur de recherche (*Google News*), puis d'accélérer les mises en forme de ces derniers pour permettre un traitement spécifiquement par IRaMuTeQ. Le nom GnOSIE signifie « *Google news Optimization to Study with Iramuteq Environnement* ». Il a été développé en langage *JavaScript* sur la plateforme *Node.js* et sous « licence MIT » à partir de briques déjà existantes. Il est en grande partie fonctionnel bien qu'encore instable et a pu être employé dans le cadre de cette recherche pour flécher une partie de l'analyse. Néanmoins, il dispose de limites : l'absence d'interface et de fonction d'extraction des résultats ainsi que le caractère semi-automatique du logiciel. Son souci majeur est qu'il ne permet pas non plus pour le moment de dépasser les limites du moteur de recherche cible²⁷⁹. Du coup, cela introduit de la latence dans le travail de constitution de la base de données. L'outil avait pour but de disposer d'un outil léger et *open source* qui permette de collecter, rassembler et de mettre en forme une vaste quantité de documents afin de former des corpus d'étude pour le logiciel. Son bilan est globalement mitigé. Avec une solution payante²⁸⁰, une recherche du même type pourra se passer de ce type de travail palliatif et de dépasser toutes les limites techniques introduites par les outils employés qui comportent une très grande majorité de logiciels libres.

²⁷⁸ Ce qui concerne donc uniquement le corpus 5 de l'analyse logométrique.

²⁷⁹ Par exemple, *Google News* ne permet pas à l'utilisateur d'afficher l'ensemble des résultats mais seulement d'afficher les 1000 premiers résultats obtenus, quelle que soit la requête.

²⁸⁰ Par exemple, avec un logiciel comme WordStat de la société Provalis.

C – A la recherche de l'objet scientifique « cyber » en France : de la communauté discursive à la communauté épistémique ?

Ce dernier volet de l'approche plurale du phénomène « cyber » se fonde sur les résultats d'une observation participante en tant que jeune chercheur dans la communauté dite « cyber » en France. Cette communauté est ici désignée en référence au phénomène linguistique « cyber ». Le concept de communauté sera notamment mobilisé de manière empirique comme un outil d'analyse du phénomène linguistique que nous cherchons à étudier. Comme souligné dans nos propos introductifs, cette recherche a débuté en octobre 2012. Le 23 novembre 2012 à Paris, j'ai assisté à la journée « Réflexions plurielles sur le cyberconflit » qui marque le début d'une première phase d'exploration du terrain²⁸¹. Couplé à un travail de veille, trois types d'évènements majeurs marqueront cette première période et ont constitué de véritables portes d'entrée dans la communauté :

1. A partir de novembre 2012 : les réunions puis les activités du groupe animant la Chaire de cyberdéfense et cybersécurité Sogeti Thalès, basée aux écoles de Saint-Cyr Coëtquidan.
2. A partir de février 2013 : les travaux du groupe de réflexion sur les données personnelles du réseau Trans-Europ Experts dans le cadre d'un projet de règlement de l'Union Européenne sur les données personnelles.
3. A partir de mars 2013 : les travaux et les évènements du séminaire jeunes chercheurs de la Chaire Castex en cyberstratégie basée à l'IHEDN en partenariat avec l'Institut Français de Géopolitique Paris 8.

Outre ces événements particuliers par leur nature, la thèse s'est enrichie d'une observation réalisée au cours d'une trentaine de colloques, ainsi que d'entretiens (dont les listes respectives figurent en annexes). Dans une seconde phase de la recherche à partir de novembre 2014, le fait d'avoir pu assister au processus de création de la chaire de cyberrésilience aérospatiale de l'armée de l'Air en partenariat avec les sociétés Dassault et Thalès aura constitué une nouvelle situation d'observation venant enrichir le terrain de nouveaux évènements. Avec un point de départ académique, l'observation se positionne dans

²⁸¹ Avec la Chaire de cyberdéfense et cybersécurité Sogeti Thalès, dans le cadre du programme du GERN - Groupe Européen de Recherches sur les Normativités - Laboratoire CESDIP - CNRS/UVSQ/Ministère de la Justice

cette recherche à la croisée des chemins entre les milieux de l'enseignement supérieur civil ainsi que militaire, de la recherche, de l'industrie et de l'administration régaliennes dans trois secteurs particuliers que sont les affaires étrangères, l'intérieur et la défense.

La posture adoptée dans les premiers temps de cette recherche a été celle du jeune doctorant, véritable rôle de composition, pour lequel j'avais la chance d'être situé à Rennes et de pouvoir me rendre souvent à Paris ce qui a permis de suivre les développements majeurs de la communauté entre la capitale et ce qui est depuis devenu « le pôle breton ». Cette posture a quelques avantages mais aussi quelques limites. D'une part, le doctorat est un travail à vocation temporaire qui place le doctorant dans une position « précaire » vis-à-vis de ses interlocuteurs. D'une part, en tant que « jeune », qui « fait des études », il bénéficie d'une forme de bienveillance qui lui procure l'important « droit d'apprendre » les codes des différents milieux auxquels il sera confronté. Du point de vue des désavantages, le fait de ne posséder aucune étiquette au départ instille une forme de méfiance eu égard à des thématiques qui sont souvent considérés comme « sensibles » par les acteurs de la communauté. De fait, il aura semblé plus efficace en termes d'accès au terrain de cumuler la qualité de doctorant avec la qualité d'employé de l'un des acteurs de la communauté. Cette solution dépasse le cas personnel puisqu'elle concerne également les autres doctorants et jeunes docteurs les mieux insérés dans la communauté qui ont pris cette qualité, parfois très tôt dans leur parcours doctoral (par exemple au travers d'un financement ou au travers d'un contrat de travail).

Pourtant, les événements observés peuvent difficilement être caractérisés comme producteurs de connaissance en eux-mêmes. Ils ressemblent davantage à des lieux de valorisation et de socialisation entre tous les milieux qui participent d'une communauté dont il est difficile de cerner les limites. En effet, la communauté « cyber » française est une forme de creuset assez inégal où convergent de nombreux acteurs issus de milieux de nature très différentes voire parfois « antagonistes ». Il y a des milieux institutionnels principalement régaliens (police, diplomatie, armées, justice). Il y a les milieux économiques et financiers avec les différents acteurs privés plus ou moins concernés par les enjeux de l'information. On trouve également des milieux militants. Et enfin des milieux académiques. Evidemment, ces milieux ne sont pas des ensembles fermés et communiquent entre eux. Il y a parfois des hybridations parmi les acteurs : les « *think tank* » qui sont des acteurs privés tournés vers la production de connaissance. Il en va de même pour les écoles militaires, structure militaire dont la mission particulière les inscrit dans un fort lien avec le monde académique. Cette

communauté est vaste et plurale. Chaque type de milieux présente différents codes et augmente le coût d'entrée du chercheur en découverte sur l'objet qui doit alors être accepté par des industriels, par les armées, par la police, par l'administration, par les hackers, et commencer à apprendre à situer lui-même dans l'univers de la recherche. Se pose néanmoins la question de « la » communauté. En présence d'organisations si éparses comment catégoriser la communauté ?

1 – La communauté : concept polymorphe.

Parler d'une communauté ici ne va pas de soi tant celle-ci a fait l'objet d'appropriations académiques diverses qui varient non seulement en fonction des champs disciplinaires, mais également en fonction des référentiels linguistiques concernés. La communauté a deux utilités : penser le lien entre l'individu et la société, penser une forme de continuité dans la transformation de ce lien. Au-delà des fondements du concept de communauté, se pose la question de sa vocation à décrire le réel et de son statut épistémologique comme base d'études empiriques. La communauté décrit-elle un ensemble concret ou l'idéal-type du groupe social étudié ?²⁸² Ce caractère opérable pose un problème car la communauté peut être rangée parmi les « concepts polymorphes ». Celle-ci a connu de nombreuses acceptations, notamment dans les *communities studies* anglo-saxonnes²⁸³.

Le concept de communauté renvoie à l'idée de la division entre individu et société, laquelle a fait l'objet de nombreux travaux sur lesquels le présent développement n'a pas pour finalité de revenir. La communauté est particulière en ce sens qu'elle fait partie des concepts qui traduisent une forme de changement entre communauté et société. La transition d'un modèle à l'autre sert de grille de lecture aux phénomènes sociaux. Cette division est attribuée principalement à la division entre *Gemeinschaft* (« communauté ») et *Gesellschaft* (« société ») proposée par Ferdinand Tönnies en 1887²⁸⁴. Ces catégories formelles opposent chez l'individu les liens affectifs préexistants issus de la « volonté organique » (*Wesenwille*), et ceux rationnels issus de la « volonté réfléchie » (*Kürwille*). La communauté reste ainsi liée

²⁸² Sur le statut de la communauté et son rôle comme base empirique, voir notamment MACIVER Robert M., *Community*, Londres, Macmillan, 1924, 446 p.

²⁸³ Voir l'analyse sur les *communities studies* : SCHRECKER Cherry, *La Communauté. Histoire critique d'un concept dans la sociologie anglo-saxonne*, Paris, L'Harmattan, 2006, 283 p.

²⁸⁴ TÖNNIES Ferdinand (1887), *Communauté et société : catégories fondamentales de la sociologie pure*, Paris, PUF, sept. 2015, 336 p.

par un sentiment d'appartenance malgré les séparations, les individus en société demeurent séparés quels que soit les mécanismes d'union. A cette première division, s'ajouteront les concepts d'association et d'union qui permettront à l'auteur de décrire une évolution vers une société individualiste et de mettre en avant l'union comme mode de recréation d'une pseudo-communauté aux travers de mécanismes de redistribution. La division est reprise par Max Weber à travers les concepts de « communalisation » (*Vergemeinschaftung*) et de « sociation » (*Vergesellschaftung*)²⁸⁵. Le premier concept décrit une relation sociale basée sur un sentiment d'appartenance et l'autre sur un compromis d'intérêts communs. Chez Durkheim, les concepts les plus proches de la communauté et de la société, sont les solidarités mécaniques et organiques²⁸⁶. Ces concepts illustrent également le passage d'une société traditionnelle (solidarité mécanique) vers une société moderne (solidarité organique). Une société traditionnelle se construit principalement sur la proximité des individus à la fois en termes géographiques et en termes sociaux. Là, où la solidarité organique se construit sur une forte spécialisation des individus et une logique de coopération.

De manière insatisfaisante, nous retiendrons que le terme communauté est généralement utilisé pour décrire les sociétés et les groupes sociaux dans le cas où ils sont appréhendés du point de vue de la participation à une forme de vie commune des individus et des institutions qui les composent²⁸⁷. Une communauté presuppose ainsi des dimensions internes et externes ainsi que des frontières qui en détermine l'appartenance. Il nous revient de questionner les frontières dudit domaine pour déterminer l'appartenance des acteurs ou non à la communauté. Une communauté est formée « indépendamment de la volonté de ses membres et sans qu'ils décident de leur implication, ce qui la distingue de l'association ou de la société »²⁸⁸. Pour cette raison, la communauté n'est pas un espace social organisé, comportant un ensemble de personnes totalement identifié unies dans un sens univoque. Elle peut être configurée de cette manière, mais ce n'est pas ce qui la détermine. En tant que groupes de personnes et d'organisations unis par un intérêt dans la connaissance du

²⁸⁵ WEBER Max (1921), *Economie et société, tome 1 : Les Catégories de la sociologie*, Paris, Pocket, janvier 2003, 410 p.

²⁸⁶ Voir notamment DURKHEIM Emile (1893), *De la division du travail social*, Paris, PUF, coll. Quadrige, 2007, 416 p.

²⁸⁷ HILLERY George A. Jr. « Definitions of Community : Areas of Agreement », *Rural Sociology*, vol. 20, n° 1, 1995, pp. 111-123

²⁸⁸ JACQUIER Claude, « Qu'est-ce qu'une communauté ? En quoi cette notion peut-elle être utile aujourd'hui ? », *Vie sociale*, 2011/2 (N° 2), p. 33-48.

cyberespace, la communauté dont nous parlons n'a pas vocation à incarner seulement une dimension scientifique car la communauté « cyber » ne peut pas être décrite comme un réseau de chercheurs œuvrant sur des thématiques communes de recherche qui n'aurait que pour vocation de diffuser des informations. Ce ne sont pas non plus des projets de recherche (même s'ils existent au sein de la communauté). Ce ne sont pas non plus des équipes de travail destinée à fournir un bien ou un service. Qu'est-ce que cette communauté ? Analyser cette communauté revient à se poser les questions de sa délimitation, de son objet, de ses modes de fonctionnement par rapport à la connaissance afin de poser la question de sa qualification au-delà du discours.

2 – La communauté discursive : situer la communauté dans l'espace sémantique.

Dans l'espace sémantique, la communauté peut être décrite comme l'espace de circulation de l'idée composé des individus et des institutions qui y concourent²⁸⁹. Inspirée de la sociolinguistique, la communauté discursive traduit ainsi une préoccupation commune articulée par des faits de langage et la production d'un lexique commun. Cette définition reprend le concept de communauté discursive (*Discourse Community*) du sociolinguiste Martin Nystrand. Cette communauté se distingue de la communauté linguistique (même langue), de la communauté de communication (même règles de déroulement et d'interprétation) et de la communauté rhétorique (même lexique) qu'elle englobe toutes trois²⁹⁰. Ce concept est notamment repris par les travaux sur le genre de John Swales²⁹¹. Selon lui, la communauté discursive comprend : la présence de finalités communes partagées ; l'existence de mécanismes d'intercommunication interne impliquant un mécanisme participatif tourné avant tout vers la diffusion de l'information et le « feed-back » avec l'utilisation d'au moins un genre communicatif mobilisé à ces fins informatives (utilisation tendant vers l'appropriation) ; l'emploi d'un lexique spécifique ; et enfin, l'existence d'experts au sein du groupe. Nous considérerons ainsi la communauté « cyber » en France comme disposant d'un lexique spécifique tourné vers la promotion de l'idée de sécurité pour l'information. Pour laquelle, grâce à la caution de différents experts issus notamment mais pas

²⁸⁹ Jean-Claude Passeron ne se réfère à la communauté que pour décrire la communauté scientifique. PASSERON, op-cit.

²⁹⁰ NYSTRAND Martin *The structure of written communication: Studies in reciprocity between writers and readers*. Orlando, FL: Academic, 1986, 234 p.

²⁹¹ SWALES, John M. *Genre Analysis: English in Academic and Research Settings*. Cambridge, Cambridge University Press, 1990, 286 p.

seulement des milieux académiques, elle mobilise les outils scientifiques de valorisation de la connaissance qu'elle finit par s'approprier.

Toutefois, cette communauté discursive ne peut recouvrir que la communauté relative au phénomène linguistique particulier « cyber ». Afin de rendre compte de l'idée médiatisée par le langage (la sécurité de l'information), il faut employer une version du concept de communauté qui intègrent le discours comme l'une des postures relatives à un objet mutuellement compris. Est-il possible de voir émerger par le discours, un autre type de communauté que la communauté discursive ? Autrement dit, la communauté discursive peut-elle s'enrichir des propriétés d'une autre forme de communauté ? Cette question aux accents théoriques a le mérite d'introduire celle du rapport de la communauté à sa propre production. Or, la communauté discursive ne permet pas d'interroger la valeur de la production communautaire. Une communauté à caractère scientifique produit immanquablement du discours. Toutefois dans la logique de la communauté discursive, le discours, même scientifique, ne correspond qu'à un genre communicatif. Certes, sa production et sa valorisation impliquent une forme de participation et de régulation qui favorise la diffusion et l'évaluation de l'information en permettant une boucle de rétroaction tout en ayant des experts tout désignés pour assurer ces mécanismes. Néanmoins, dire qu'une communauté possède un caractère scientifique implique un rapport particulier à la connaissance qui devrait être son amélioration, et pas simplement une simple diffusion. Toute méthode scientifique qu'elle soit moniste, pluraliste, positiviste, critique, post-positiviste (...) s'inscrit par rapport à l'objectif de produire de la connaissance (y compris lorsqu'elle est mobilisée pour défendre l'idée de son impossibilité). Le rapport de la société à la connaissance détermine globalement la valeur de l'activité de recherche. Cette valeur peut être caractérisée dans un rapport de finalité soit d'un point de vue intrinsèque à l'activité poursuivie par la communauté, soit d'un point de vue extrinsèque par le pouvoir d'influence de cette communauté.

3 – La communauté épistémique : production et influence communautaires.

La communauté épistémique a pour origine intellectuelle le concept d'épistème de Michel Foucault décrit dans *Les Mots et les Choses*²⁹². Ce qu'il est « possible de dire » est déterminé par des conditions de vérité qui varient historiquement. Ces conditions forment

²⁹² FOUCAULT Michel, *Les mots et les choses : une archéologie des sciences humaines*, Paris, Gallimard, 1966, 405 p.

l'*épistèmè*. Le concept fait la part belle au discours relatif à un objet dans la mesure où l'objet est ce qu'en dit celui qui en parle. Michel Foucault le mobilise principalement pour analyser la transformation qui se réalise dans un contexte donné. Ainsi l'*épistèmè* s'écarte d'une histoire des idées continue en ce qu'il fait la part belle à l'analyse des discontinuités entre deux régimes de vérité. Sur le point de cette discontinuité, elle s'oppose également au structuralisme en ce que ce dernier suppose à la fois une transformation et un invariant²⁹³. C'est ici tout l'intérêt de l'*épistèmè* appliqué à la communauté. Là où la communauté discursive fait la part belle à la structure du discours comme outil d'analyse, la communauté épistémique permet d'abandonner le langage au profit de l'enjeu. Dès lors la communauté épistémique restitue la place du phénomène du langage dans un ensemble plus vaste : celui de la sécurité de l'information.

Le concept de communauté épistémique permet d'interroger le rôle de l'expert dans la décision publique ainsi que l'influence internationale sur la communauté considérée. Plusieurs définitions existent. La plus ancienne est employée pour décrire l'importance sociétale accordée à la méthode scientifique dans un rôle de production de la vérité²⁹⁴. Une communauté épistémique est ainsi la communauté de travail où l'intérêt épistémique prime sur toute autre intérêt.

La communauté épistémique est caractérisée par une expertise et une compétence reconnue dans un domaine particulier, et elle peut faire valoir un savoir pertinent sur les politiques publiques concernant le domaine en question²⁹⁵. Elle est introduite dans les Relations Internationales notamment par Peter Haas dans un numéro spécialement dédié de la revue *International Organizations* autour de plusieurs principes organisateurs²⁹⁶ : un socle commun de croyances sur les principes et les normes, les origines et les solutions d'un

²⁹³ En complément, voir à ce sujet SCHLANGER Nathan. « 8. Piaget et Leroi-Gourhan. Deux conceptions biologiques des connaissances et des techniques », In LATOUR Bruno et LEMONNIER Pierre (éd.), *De la préhistoire aux missiles balistiques. L'intelligence sociale des techniques*. La Découverte, 1994, pp. 165-184.

²⁹⁴ Voir HOLZNER Burkart, *Reality Construction in Society*. Cambridge: Mass., Schenkman Pub. Co 1968, 192 p ; HOLZNER Burkart and MARX John H., *Knowledge Application: The Knowledge System in Society*, Boston, Allyn & Bacon, 1979, pp. 107-111

²⁹⁵ HAAS Peter M. « Introduction: Epistemic communities and international policy coordination », *International Organization*, vol. 46(1), 1992, pp. 1-35. Le numéro entier de la revue est dédié aux communautés épistémiques. Voir aussi la conclusion dudit numéro ADLER Emanuel et HAAS Peter M., « Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program », Ibid. pp. 367-390.

²⁹⁶ Ibid, p. 3

problème, des critères de validité du savoir, des propositions d'action publique associées aux problèmes. Dans l'approche de Haas et d'Adler, la communauté épistémique revendique l'autorité en matière de connaissances et de leurs applications à la politique. Autrement dit, il s'agit d'une communauté à la fois concernée par la production de connaissance et l'influence du politique. Les premières études concernant les communautés épistémiques se sont souvent concentrées sur des groupes de scientifiques en interrogeant des cas uniques sans avoir recours à des ensembles plus larges d'acteurs que des groupes de techniciens ou de scientifiques²⁹⁷. A partir du milieu des années 2000, les travaux ont évolués pour inclure d'autres types de groupes ainsi que des travaux comparatifs. C'est notamment le cas des publications de Mai'a Cross²⁹⁸, de Nuhket A. Sandal²⁹⁹ ou encore des publications plus récentes d'Emanuel Adler³⁰⁰.

Dans cette recherche, le phénomène linguistique « cyber » est principalement le fait d'une communauté discursive, laquelle participe d'une communauté épistémique plus large. Cependant les travaux qui analysent une communauté à caractère scientifique opèrent le plus souvent une transition entre communauté de pratiques et communauté épistémique³⁰¹. Cette transition a également court dans les autres disciplines académiques qui mobilisent la communauté épistémique pour analyser la production scientifique par exemple en sciences de gestion³⁰². Le problème de la communauté de pratiques pour comprendre le phénomène linguistique « cyber », c'est qu'elle nécessite une forme d'histoire commune liée à leur

²⁹⁷ Par exemple : HAAS Peter M. « Do regime matter? Epistemic community and Mediterranean Pollution Control », *International Organization*, vol. 43 (3), 1989, pp. 377 – 403. ALDER Emanuel, « The emergence of cooperation: national epistemic communities and the international evolution of the idea of nuclear arms control », op-cit. 1992 pp 101 - 145.

²⁹⁸ Notamment CROSS Mai'a K. Davis, *The European Diplomatic Corps: Diplomats and International Cooperation from Westphalia to Maastricht*, Palgrave Macmillan, 2007 224 p.

²⁹⁹ SANDAL Nuhket A., « Religious Actors as Epistemic communities in Conflict Transformation: the cases of South Africa and Northern Ireland », *Review of International Studies*, n° 27 (3), 2011, pp. 929 – 949.

³⁰⁰ ALDER Emanuel et POULIOT Vincent, « International Practices », *International Theory*, n°3 (1), 2011, pp.1-36.

³⁰¹ Voir notamment AKRICH Madeleine, « From Communities of Practice to Epistemic Communities: Health Mobilizations on the Internet », *Sociological Research Online*, vol. 15, no. 2, 2010, pp. 1–17; ainsi que pour une synthèse MEYER Morgan, et MOLYNEUX-HODGSON Susan « « Communautés épistémiques » : une notion utile pour théoriser les collectifs en sciences ? », *Terrains & travaux*, vol. 18, no. 1, 2011, pp. 141-154.

³⁰² Voir par exemple COHENDET Patrick, CREPLET Frédéric, et DUPOUËT Olivier. « Innovation organisationnelle, communautés de pratique et communautés épistémiques : le cas de Linux », *Revue française de gestion*, vol. n° 146, no. 5, 2003, pp. 99-121.

pratique professionnelle³⁰³. Le présent rejet du concept de communauté de pratiques tient à l'absence de cette histoire professionnelle commune à la fois du point de vue du discours comme de l'enjeu décrit.

Cet enjeu idéal s'inscrit dans notre approche de la sécurité comme en dehors de mesures politiques précises cela nous conduit à exclure les méthodes propres à l'analyses des politiques publiques telles l'*advocacy coalition framework* (ou ACF) malgré une ressemblance avec la communauté épistémique³⁰⁴.

Celle-ci est comprise comme la communauté transnationale dont les membres experts scientifiques ou non, au service des États ou non, concourent à la transformation de l'information en enjeu de sécurité peu importe leur affiliation discursive. Elle sera abordée à travers l'élargissement du concept proposé par Mai'a Davis Cross en 2013 à partir de la définition de Peter Haas³⁰⁵. Cette définition met l'accent sur l'influence de la communauté à travers sa cohésion interne (Ontologiquement, les acteurs peuvent être gouvernementaux ou non, scientifiques ou non). L'intérêt épistémologique de la communauté épistémique réside principalement dans les processus relatifs à la globalisation³⁰⁶. Ces processus de plus en plus complexe nécessite le recours à l'expertise pour pouvoir être menés du fait de leurs enjeux multiples. Cela est d'autant plus vrai dans le cadre des approches transnationales des problèmes internationaux. Dès lors cette communauté épistémique nous permet d'interroger l'influence internationale sur la sécurisation de l'information. Évidemment, la communauté épistémique ne forme pas un ensemble unifié.

La base de cette approche revient à dépasser la seule question de l'existence de la communauté épistémique pour parvenir à questionner son influence. Une communauté épistémique peut être forte ou faible dans le contexte de ses relations avec les autres acteurs. Cela dépend en grande partie de sa cohésion interne et notamment de son caractère « professionnel ». Le professionnalisme d'une communauté ne s'entend pas au sens d'un

³⁰³ WENGER Etienne, *Communities of Practice: Learning, Meaning, and Identity*, Cambridge University Press, 1999, 318 p.

³⁰⁴ SABATIER Paul A. « Advocacy coalition framework (ACF) », In. BOUSSAGUET Laurie (éd.), *Dictionnaire des politiques publiques. 3e édition actualisée et augmentée*. Presses de Sciences Po, 2010, pp. 49-57.

³⁰⁵ CROSS Mai'a K. Davis. « Rethinking Epistemic Communities Twenty Years Later. », *Review of International Studies*, vol. 39 n°01, 2012, pp. 137–160.

³⁰⁶ Sur la globalisation de manière plus étendue voir l'ouvrage collectif : HELD David, et al. *Global Transformations: Politics, Economics and Culture*. Cambridge, Polity Press, 2001, 602 p.

corporatisme mais des éléments de cohérence interne statuaires, interactionnels, protocolaires et identitaires : sélection et entraînement des membres, fréquence et qualité des rencontres, des normes partagées et une culture commune. Cela dépasse la simple notion de profession. Ces critères ne fondent pas l'existence de la communauté mais décrivent sa capacité d'influence nominale.

Cette définition de l'influence communautaire repose sur un principe d'incertitude (*uncertainty*) qui fonde un espace dans lequel la communauté peut exister et permet d'en restituer la portée qu'importe les conditions de certitude ou d'incertitude qui animent le contexte de l'objet. Là où la communauté épistémique est généralement entendue dans une perspective *a posteriori* d'une décision ou d'une crise. L'approche de Mai'a K. Davis Cross mobilise celle-ci comme étant un élément perpétuel sinon permanent de la vie internationale. L'influence d'une communauté ne diminue pas une fois que ses idées ont été prise en compte par la décision politique. Cette prise en considération renforce et alimente la communauté. De même, les mutations du contexte peuvent également influencer la production de connaissance de la communauté et la voir adopter des idées qu'elle récusait précédemment³⁰⁷. Il faut ainsi séparer l'existence de la communauté de son influence concernant une politique particulière dont la progression peut également être graduelle, voire décliner. Cela entraîne la séparation de l'activité de production de connaissance de l'influence de la communauté.

Cette particularité conduit à rejeter les catégories produites au travers du lien organique de la communauté. Dans la question de savoir si une communauté existe ou non, il faut dépasser le fait de savoir si une communauté épistémique est le résultat d'une volonté régaliennes ou d'une organisation non-gouvernementale. Les interactions entre les membres de la communauté sont davantage révélatrices que le « rôle bureaucratique » qui leur est attribué.

Enfin le dernier apport de cette définition intéresse le caractère scientifique de la connaissance produite. Mai'a K. Davis Cross fait ici mention des travaux de William J. Drake et Kalypso Nicolaïdis³⁰⁸. Lesquels affirment que la communauté épistémique se construit au-

³⁰⁷ Sur ce dernier point, l'auteure se réfère ici à l'étude : PIERSON Paul, « Increasing Returns, Path Dependence, and the Study of Politics », *American Political Science Review*, n°94 (2), 2000, pp. 251 – 267.

³⁰⁸ Toujours dans le numéro d'*International Organization* dirigé par Haas et voir DRAKE William J., et NICOLAIDIS Kalypso. « Ideas, Interests, and Institutionalization: ‘Trade in Services’ and the Uruguay Round. » *International Organization*, vol. 46, no. 1, 1992, pp. 37–100.

delà de toute affiliation institutionnelle de ses membres par les croyances communes de ces derniers dans les origines et les solutions d'un problème qui leurs apparaissent « scientifiquement objectives ». Des « scientifiques », peuvent ainsi former des communautés épistémiques, mais également sans que cette liste ne soit limitative : des journalistes, des haut-fonctionnaires, des spécialistes de l'industrie, des avocats... La connaissance scientifique joue ici le rôle de « glue » qui maintien la cohérence de la communauté et lui permet de se défendre contre ses adversaires³⁰⁹.

L'articulation entre communauté discursive et communauté épistémique interrogera à l'aune de notre analyse le rapport du phénomène linguistique à l'enjeu qu'il revendique : celui de la sécurité de l'information. Cela permettra de mettre en avant la production de connaissance qui dépasse ce seul phénomène pour englober un enjeu beaucoup vaste, ainsi que les limites techniques, nationales et conceptuelles du phénomène en question. Autrement dit, à travers la communauté épistémique nous faisons du cyberspace et des termes dérivés une ligne parmi bien d'autres où les frontières du discours traceront les grandes oppositions communautaires et y mettront en lumière les phénomènes d'influence.

Section 4 – Entre phénomène discursif et combinaison pragmatique, l'apport d'une méthode de travail abductive.

Plus qu'un simple raisonnement logique additionnel qui viendrait s'ajouter à l'état de l'art. Dans le contexte particulier de cette recherche, l'abduction permet au quotidien une pratique du travail entre deux opérations de recherche finalisée. D'un côté, se trouve la compréhension du phénomène au travers d'une épistémologie du discours qui fonde une approche phénologique plurale/ L'autre opération de recherche vise la construction d'un texte explicatif idéal fondé sur une combinaison des théories répondant à des questions posées par le phénomène. L'abduction suppose un mode de raisonnement construit autour de la révision constante des attentes théoriques par le biais de l'observation. Elle se distingue de l'induction qui confronte le résultat obtenu à la théorie sur la base d'une formulation d'énoncés généraux tirés de l'observation. Elle se distingue également de la déduction laquelle repose sur la confrontation d'hypothèses théoriques tirées de la littérature scientifique à la réalité

³⁰⁹ GOUGH Clair, et SHACKLEY Simon. « The Respectable Politics of Climate Change: The Epistemic Communities and NGOs » *International Affairs*, vol. 77, no. 2, 2001, pp. 329–345

empirique. Elle pourrait ainsi être décrite comme un raisonnement d’induction-déduction dont la démarche vise l’application d’un corpus théorique déjà développé (déduction) à un objet nouveau (induction)³¹⁰. D’une première inférence abductive, il faut ensuite opérer une déduction des conséquences de cette hypothèse qui doivent être vérifiée. L’abduction se traduit ainsi par l’observation d’un cas singulier, l’inférence du lien entre cette occurrence et la théorie générale, la formulation d’une hypothèse puis de confronter celle-ci à la réalité empirique. Cette méthode de travail implique ainsi des préconceptions guidant une définition préliminaire de l’objet puis de proposer une explication plausible. Toutefois, celle-ci pour être complète se doit d’introduire une boucle récursive dans le raisonnement entre l’explication et la réalité empirique. S’inspirant du pragmatisme, cette pratique est ainsi destinée à lier l’approche discursive de l’objet et la combinaison pragmatique conduite par les problèmes. Dans le dialogue entre un pragmatisme et approche discursive, cette recherche mobilise l’abduction pour nourrir la démarche érotétique qui sert de socle épistémologique à la combinaison ainsi que l’approche phénoménologique de l’objet. Afin de parvenir à cette combinaison, il s’agit de mettre en place une boucle récursive entre les idées marquées par le discours et les problèmes qu’ils soulèvent. Ces itérations entre discours et théories par l’intermédiaire des questions ont progressivement participé à la définition et à la délimitation de ces dernières. L’objet de recherche constitué par la définition de ces questions est donc construit tout au long de la recherche. Cette précaution nous semble nécessaire pour travailler une notion en prolifération qui ne constitue pas un objet formalisé. En effet, il n’y qu’à

³¹⁰ L’abduction a été inventée par Charles Sanders Pierce, l’un des fondateurs du pragmatisme philosophique pour servir de lien entre les deux approches. PIERCE Charles S. « On the Natural Classification of Arguments », *Proceedings of the American Academy of Arts and Sciences*, vol. 7, 1867, pp. 261–287.

observer l'évolution de la notion et des normes entre le début de la recherche et la fin de la période de recueil des données afin de caractériser une évolution hebdomadaire de la notion. Ce manque de stabilité de la notion n'aura guère contrebalancé son actualité, laquelle peut entraîner le chercheur dans une spirale d'informations contradictoires. À travers la veille sur l'actualité, ce n'est pas moins de 400 articles de presse qui ont été collectés sur les deux premiers mois de la thèse (qui sont bien loin de représenter la totalité de la presse française dédiée au sujet publié sur la période de ces deux mois).

Il y a donc un effet de masse difficile à appréhender en termes de données à trier. En comparaison, un ensemble formalisé tel que les théories des Relations Internationales ou plus généralement la Science Politique semblent connaître une évolution bien plus lente, avec tous les avantages et désavantages déjà mentionnés. Ainsi le premier ensemble théorique guide la lecture de l'actualité de l'objet, tandis que celle-ci vient interroger la pertinence des

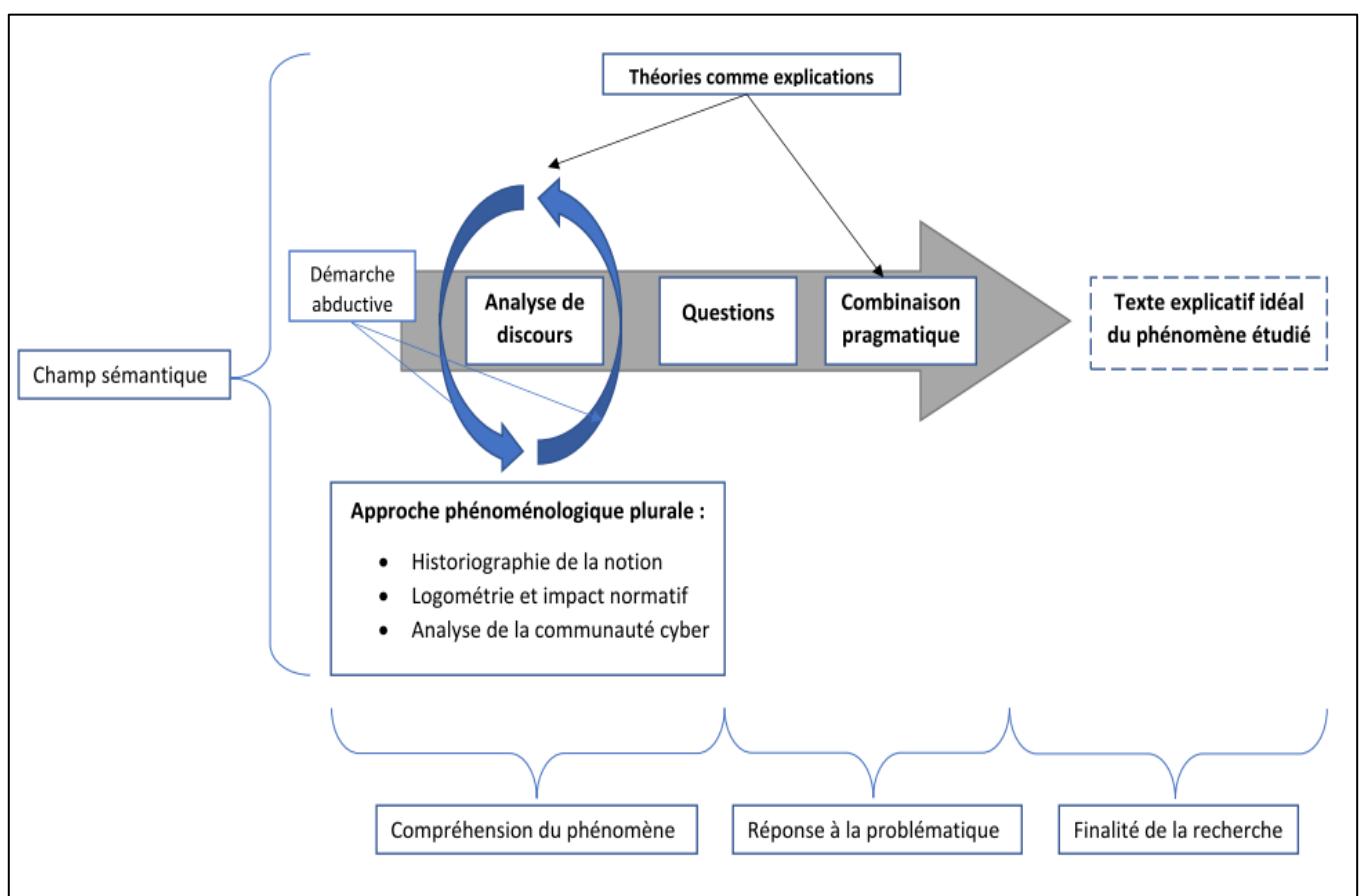


Figure 3 – Processus de recherche global avec ajout de la démarche abductive

explications proposées. Pour appréhender numériquement cette masse d'information et l'impératif de tri, le corpus n°4 de notre étude qui comprend l'ensemble des publications francophones de presse généraliste et spécialisée entre 2001 et 2016 contenant le mot cyberespace ou un terme dérivé disponibles sur la plateforme Factiva (plutôt orienté presse locale) comprend 22643 textes sélectionnés (sur 45221 résultats identifiés). Le corpus N°5 quant-à-lui, qui est la même chose à partir de Google News, comprend 73662 textes sélectionnés (sur 201362 résultats identifiés).

La démarche abductive peut être ajoutée pour établir notre compréhension du phénomène étudié car elle fonctionne dans un référentiel qui est l'espace sémantique entre le langage naturel et le langage académique³¹¹. Retranscrite dans ce cadre (Fig. 3), l'abduction constitue un moyen de circulation des idées entre notions et concepts qui forment le socle sur lequel se construit cette recherche. La circulation s'établit entre les théories mobilisées qui ont une composante sémantique et l'approche phénoménologique qui a pour fonction d'y inclure les données du phénomène politique afin de produire l'analyse de discours. La réponse à la problématique se situe dans les questions posées par le discours auxquelles les théories répondent dans une optique combinatoire³¹² afin de contribuer au texte explicatif idéal qui constitue la finalité de la recherche. Le processus de recherche vise à dépasser le caractère protéen d'un langage pour se concentrer sur les questions théoriques qu'implique l'idée soutenue par ce même langage. Elle opère un détour dans la question posée car la recherche n'interroge pas le sens d'un phénomène dans une discipline académique, mais les réponses apportées par celle-ci aux questions que le phénomène pose.

Combinant une épistémologie du discours inspirée de Jean-Claude Passeron et le modèle de combinaison pragmatique conduit par les problèmes de Jérémie Cornut avec une méthode de travail abductive, ce processus de recherche répond à plusieurs questions relatives à l'objet de cette thèse et à la méthodologie employée. C'est un processus qui permet de traiter les données du phénomène discursif sur un plan similaire (champs sémantique) aux concepts posés par les théories. L'analyse de discours traduit le phénomène discursif en objet sémantique. De même, ce processus répond à la question de la sélection érotétique dans le pragmatisme conduit par les problèmes. C'est l'analyse de discours qui fonde l'intérêt des

³¹¹ PASSERON, 1991, op-cit.

³¹² CORNUT, 2012, op-cit.

questions retenues. Enfin, ce processus permet de s'extraire de la subjectivité du discours et de l'acteur par la mise en relief du contenu idéologique du discours.

Une telle démarche inscrit le chercheur au centre de logique d'observation de co-construction de l'objet de sa recherche. Cela interroge l'influence de la perception du chercheur sur le résultat de la recherche. Il ne s'agit pas de tenter de défendre le mythe de la neutralité axiologique³¹³. Mais ce positionnement implique de trancher les conflits entre une aspiration d'objectivité propre à toute démarche à caractère scientifique et la prise en compte de la subjectivité des objets que nous avons déjà souligné ainsi que du contexte particulier de la recherche. Il ne s'agira pas non plus de revenir sur le paradoxe de l'effet de légitimation de l'analyse d'un enjeu de sécurité, y compris lorsque celle-ci adopte un point de vue critique. Pour partie, ces interrogations ont déjà été évoquées sous une forme ou une autre dans le cadre théorique du projet.

Section 5 – Du doctorant à l'officier : regard critique sur un parcours doctoral engagé.

Au-delà de la seule écriture de cette thèse, il s'agit principalement de s'interroger sur le rapport du chercheur à son propre terrain à la fois dans les biais et dans leurs influences réciproques. Outre les débats précédemment évoqués, cette question de l'engagement du chercheur est principalement l'objet des approches sociologiques. Ce questionnement interroge le but et la morale du chercheur ainsi que les effets induits de son travail sur l'objet qu'il analyse. Bien que l'engagement de la personne du doctorant fasse partie en tant que valeur de la formation, dont il constitue l'une des spécificités notamment à travers les chartes de thèse. L'engagement du terrain est ici perçu comme différente. Cette interrogation existe à deux niveaux de manière complémentaire : d'une part, dans la position du doctorant qui mobilise en tant que terrain une des communautés discursives dont il devient membre à travers son expertise ; d'autre part, dans un engagement particulier vis-à-vis du terrain. Cette thèse a été commencée fin 2012. En novembre 2014, le projet a bénéficié d'un engagement dans l'armée de l'air en qualité d'officier sous contrat. Une partie de la recherche a donc été

³¹³ A ce sujet, outre les œuvres de Max Weber, voir plus particulièrement la traduction de la conférence de Max Weber de 1917, intitulée « La Science, profession et vocation » dans l'ouvrage KALINOWSKI Isabelle, *La science, profession et vocation. Suivi de "Leçons wébériennes sur la science & la propagande"*, Paris, Agone, 2005, 300 p.

conduite en tant que doctorant dépourvu de toute condition militaire à l'université Rennes 1. La seconde partie a été conduite à la fois comme doctorant de l'université et comme officier au centre de recherche de l'armée de l'air (CReA)³¹⁴. Il s'agit d'une unité militaire rattachée à l'école de l'air qui accueille la quasi-totalité des enseignants-chercheurs de l'établissement³¹⁵.

L'idée de l'engagement comprise pour le chercheur comme le fait de « plonger tout entier dans l'activité quotidienne des individus qu'il observe » implique une distinction. Cette distinction est une question de degré entre le chercheur engagé « par » ou « dans » son terrain³¹⁶. Un chercheur engagé dans son terrain représente le cas classique du chercheur qui enquête auprès de son terrain à travers son observation empirique (qu'elle soit participante ou ethnographique)³¹⁷. Un chercheur engagé par son représentation le cas où le chercheur est rémunéré par tout ou partie d'acteurs présents dans le milieu étudié.

« Pourquoi faire confiance à un officier qui est aussi universitaire, et qui finalement ne serait ni l'un ni l'autre ? »³¹⁸.

Dans le contexte de cette recherche, cet engagement est double : « dans » le terrain de la communauté discursive de la sécurité de l'information, et « par » l'État français (dans l'armée de l'air) compris comme un acteur dudit terrain. C'est-à-dire que cet engagement ne saurait être compris comme dual. L'ensemble constitue deux liens à un terrain identique. C'est ce que vient qualifier l'expression de chercheur « embarqué »³¹⁹. Au-delà du lien de subordination qu'implique d'ordinaire une telle situation, il faut également introduire l'aspect particulier d'une composante du terrain : le monde militaire. Le monde militaire qualifie souvent l'institution militaire et constitue un ensemble de milieux affectés d'une

³¹⁴ Les dénominations du centre de recherche ont varié au cours de son histoire entre centre de recherche de l'école de l'air (CREA) et centre de recherche de l'armée de l'air (CReA).

³¹⁵ Civils (contractuels, détachés de l'enseignement supérieur) et militaires (de carrière et contractuels).

³¹⁶ ALAM Thomas, GURRUCHAGA Marion, O'MIEL Julien, « Science de la science de l'État : la perturbation du chercheur embarqué comme impensé épistémologique », *Sociétés contemporaines*, 2012/3 (n° 87), p. 155-173.

³¹⁷ L'observation distante au travers d'un terrain d'enquête dématérialisé n'entre pas dans l'idée d'engagement.

³¹⁸ PORTE Rémy, « Officier d'active et historien est-il indispensable d'être schizophrène ? », *Les Champs de Mars*, 2015/2 (N° 27), p. 59-66.

³¹⁹ ALAM Thomas, GURRUCHAGA Marion, O'MIEL Julien op-cit. §3.

représentation de « spécificité »³²⁰. « L'institution militaire est un moyen de l'action militaire, elle-même moyen de l'action politique, et il n'est pas judicieux de rompre le rapport entre les fins et les moyens »³²¹. En termes d'enquête, le terrain militaire implique de nombreux traits méthodologiques qui sont finalement proches des autres terrains : la gestion des méfiances, la prise en compte de la culture institutionnelle et les contraintes liées à l'échantillonnage. Le trait caractéristique du milieu militaire réside dans le fait qu'il s'agit d'un « milieu clos »³²² qui implique un « investissement » particulier « idoine » qu'il soit civil ou militaire³²³. La question de l'embarquement d'un chercheur sur ce terrain réside donc principalement dans des séries d'« épreuves de confiance » marquées par les divisions propres au terrain. La communauté discursive analysée est un terrain plural composé de divers acteurs. Cette division ontologique implique une division des débats et finalement de choisir un camp plutôt qu'un autre.

La recherche et le monde militaire sont deux mondes qui s'ignorent l'un et l'autre et ne se connaissent que peu en règle générale malgré un dialogue construit par de nombreux acteurs institutionnels et des partenariats... De la même manière que la conduite des opérations militaires représente une forme d'inconnue pour les universitaires et pour la recherche ; la majorité des officiers et des cadres ignore tout du fonctionnement interne de l'université. Il faut rajouter à cela le poids des *a priori* qui dépasse le seul cadre de la connaissance, des statuts, des hiérarchies et des emplois. « Pour l'universitaire, l'officier manquera de subtilité ou de finesse dans l'expression d'un discours peu problématisé. Pour l'officier, l'universitaire restera celui qui pose des questions sans apporter de réponse. [...] En clair, « l'Autre » appartient à une institution non seulement différente et méconnue (et à ce titre parfois crainte), mais aussi plus ou moins soupçonnée collectivement de vouloir s'attaquer à nos fondamentaux »³²⁴. Milieux hiérarchisés animés de leur propres contraintes, ces deux mondes

³²⁰ A propos du concept de spécificité militaire : BARDIES Laure, « Du concept de spécificité militaire », *L'Année sociologique*, 2011/2 (Vol. 61), p. 273-295.

³²¹ Ibid, extrait de la note n°2.

³²² PAJON Christophe, « Le sociologue enrégimenté : méthodes des sciences sociales en terrain militaire », In. GRESLE François (dir.), *Sociologie du milieu militaire : les conséquences de la professionnalisation des armées et de l'identité militaire*, Paris, L'Harmattan, 2005, pp. 45 – 55

³²³ MARTIN Clément et PAJON Christophe, « La sociologie militaire par les personnels de la défense : une sociologie d'insiders ? », *Les Champs de Mars*, 2015/2 (N° 27), pp. 23-30.

³²⁴ Ibid § 17.

ont respectivement en commun une forme d'exclusivité et la poursuite de leurs autonomies respectives.

La présence d'enseignants-chercheurs dans les établissements de formation dépendants des armées répond par ailleurs à cette dernière logique d'autonomisation à travers la certification et de la diplomation des formations³²⁵. A l'image des autres composantes de l'administration, le Ministère de la Défense, puis des Armées, constitue un contexte de la recherche qui fait naître un certain nombre d'attentes.³²⁶

C'est particulièrement le cas dans les administrations « sensibles » en général³²⁷. Au-delà des contraintes indigènes et des contraintes particulières qui pèsent sur le jeune chercheur, se pose la question de l'impact sur cette recherche. L'appartenance aura diverses des conséquences sur la mise en œuvre des techniques d'enquête, à la fois dans le recueil du matériau d'enquête et dans l'exploitation et la valorisation des données obtenues³²⁸. L'idée générale réside dans un doute sur la compatibilité avec les exigences scientifiques qui anime une forme de « soupçon »³²⁹. Ce soupçon n'est pas nécessairement interne à l'institution mais reflète l'image particulière de celle-ci à l'égard des autres acteurs ainsi que la représentation de certains acteurs dans la vision de cette institution. Par ailleurs, ce soupçon est également une forme de valorisation du travail de recherche proprement dit. Le mécanisme du soupçon repose sur une forme de paralogisme : Le doctorant est membre de telle institution. Le doctorant travaille sur ce sujet. Donc, le doctorant travaille pour l'institution sur ce sujet précis. Ce faux principe a deux corolaires : le doctorant représente l'institution sur la

³²⁵ Voir notamment HAMELIN, Fabrice. « Le combattant et le technocrate. La formation des officiers à l'aune du modèle des élites civiles », *Revue française de science politique*, vol. 53, no. 3, 2003, pp. 435-463. ; AUGÉ Axel, « La formation initiale des futures élites militaires à Saint-Cyr : un dispositif institutionnel en évolution », *Education et sociétés*, 2008/1 (n° 21), p. 81-94. ; ou encore BOËNE Bernard, « La formation initiale et sa place dans le continuum de la formation des officiers de carrière », *Stratégique*, 2017/3 (N° 116), p. 37-60.

³²⁶ « Être un personnel de la Défense, c'est s'interdire les effets d'hystérèse [...] On attend du sociologue estampillé ministère de la Défense, voire d'un sociologue militaire, qu'il se plie aux « manières d'être » afin de ne pas être discrédiété et de mener à bien son travail d'enquête. » MARTIN Clément et PAJON Christophe, op-cit. p. 26.

³²⁷ Voir notamment MONJARDET Dominique, « Le chercheur et le policier. L'expérience des recherches commanditées par le ministère de l'Intérieur », *Revue française de Science politique* n°2, 47^e année, 1997, pp. 211-225.

³²⁸ MARTIN Clément et PAJON Christophe, op-cit.

³²⁹ Ibid.

thématique de son travail aux yeux de l'extérieur. L'institution reconnaît pour elle-même une forme de valeur au travail accompli par le doctorant dans son activité et sa recherche.

Cette représentation s'avère par rapport à la réalité des thèses produites par les militaires en général. Hors quelques domaines précis où le doctorat fait partie d'un cursus professionnel identifié (« spécialité »), la plupart des thèses de doctorats réalisées par les militaires le sont sur leur temps personnel. Sauf cas particuliers, le dispositif lié au doctorat proprement dit est autonome par rapport à la vie militaire. Le doctorant paye ses propres frais d'inscription en thèse auprès d'une université et travaille sur sa recherche quand il est de repos. Statistiquement, l'échec de la thèse n'est pas un obstacle à la « carrière » du doctorant dans les forces. Pas plus que sa réussite n'offre de garantie dans la carrière d'un cadre. Au contraire, dans certains cas le fait d'opter pour un doctorat peut même parfois être dommageable à l'avancement et la carrière de certains personnels de l'institution, si celle-ci souhaite employer ces mêmes personnes à d'autres fins.

Par ailleurs aux termes d'entretiens réalisés avec plusieurs présidents de catégories³³⁰, il apparaît que le doctorat ne soit pas un niveau de qualification généralement considéré d'un point de vue des différentes directions des ressources humaines du ministère des armées. Le doctorat n'existe qu'à la marge d'une gestion particulière des postes et n'est pas intégré dans l'enseignement supérieur militaire (y compris chez les officiers de carrière). De fait, le doctorat est une composante absente du lien de rattachement entre la personne du doctorant et l'institution. Se pose alors la question du lien de rattachement à l'aune du contexte particulier de cette recherche.

Dans cette situation, être un doctorant engagé sous contrat en qualité d'officier subalterne, c'est opérer une synthèse quotidienne et individuelle des contraintes propres à chacun des deux mondes. Aux fins de réaliser cette synthèse, le doctorant dispose d'une forme d'avantage qui réside paradoxalement dans le caractère transitoire de sa situation personnelle. Celle-ci est construite et entretenue par l'absence de carrière, donc de lien de rattachement définitif à l'un ou l'autre des mondes. Toutefois, le doctorant ne saurait demeurer dans cette

³³⁰ Les présidents de catégories sont des délégués élus au sein d'une catégorie de personnel (officiers, sous-officiers, militaires du rang). Ils ont pour fonction de traiter des questions relatives aux personnels dans les domaines professionnels, social et moral. C'est un échelon de concertation de proximité. Au titre de sa définition ministérielle, « la concertation constitue le mode de dialogue spécifique aux militaires avec le ministre et ses grands subordonnés, permettant d'aborder, dans le respect des spécificités liées à l'état militaire, les sujets fondamentaux qui les concernent dans les domaines statutaires et de condition militaire. »

position un peu particulière et doit donc choisir. Bien que les situations soient toutes très différentes, on pourrait dire que ce choix se situer entre accorder de l'importance à sa thèse, ou lui en accorder moins (voire l'abandonner) au profit d'autres activités plus valorisantes vis-à-vis de l'objectif d'un contrat supplémentaire dans les forces ou des objectifs de carrières dont le doctorat est par nature exclu.

A l'échelle de cette recherche, ce recrutement a donc eu un impact sur différentes composantes du projet, notamment matérielles. Indépendamment des contraintes matérielles, certaines contraintes spécifiques à l'objet de recherche doivent également être mentionnées, car elles ont entraîné des choix importants dans le traitement des résultats obtenus.

Section 6 – Evolution des contraintes matérielles et scientifiques de la recherche.

Les contraintes liées à la thèse ont connu diverses évolutions tout à long du travail de recherche. La majeure partie des orientations du projet de recherche est le fruit de ces contraintes. La contrainte s'entend ici comme une exigence et parfois un obstacle autour desquels il a fallu construire cette recherche. Ces contraintes ne doivent pas être comprises comme des éléments statiques mais comme des ensembles structurants la recherche de manière quotidienne et dynamique. Leur mention sert deux objectifs : d'une part, elles participent de la description du projet de recherche ; d'autre part, cette mention permet la mise en valeur des choix opérés pour les contourner. Bien que ces lignes les présentent sous une forme de liste relativement succincte, il faut considérer que ces contraintes sont non seulement évolutives mais également connectées entre elles. A titre d'exemple, la question du financement du projet ne saurait être considéré totalement à part de la question de la mobilité. Ayant précédemment évoqué les contraintes épistémologiques liées à l'objet de la recherche, cette section se concentra les contraintes matérielles et les difficultés scientifiques rencontrées dans le projet.

A – Contraintes matérielles du projet

Trois types contraintes matérielles seront retenues. Elles sont liées au financement de la thèse, à la mobilité géographique et à la gestion du temps.

1 – Financement de la thèse.

La thèse a commencé comme financée « sur deniers propres » les premières années de novembre 2012 à novembre 2014. La raison principale réside dans le faible nombre de financement octroyés. Cette situation correspond alors un tiers des doctorants inscrits en thèse durant l'année 2012-2013, d'après les chiffres du Ministère de l'Enseignement supérieur³³¹. La première période de ce doctorat a été financée au travers d'une activité salariée constituée notamment des vacations à l'université, de diverses prestations de conseil, ainsi que d'une mission d'assistant de justice auprès du président du Tribunal de Grande Instance de Rennes. Au-delà du financement proprement dit, cette contrainte a pour effet de prendre du temps sur la recherche pour l'affecter à des activités qui ne profitent pas directement à l'avancement de celle-ci.

L'engagement sur un nouveau contrat professionnel à partir de novembre 2014 participe de la même nécessité. Bien que souffrant d'obligations plus fortes et plus variées, ce dernier engagement comble une partie des défauts du mode d'organisation précédent. Un poste d'officier sous contrat au centre de recherche de l'armée de l'air³³², représente sans doute l'une des meilleures *via media* entre un financement de type convention industrielle de formation par la recherche (CIFRE) et un contrat de travail. Comparable sur bien des aspects à un contrat d'attaché temporaire d'enseignement et de recherche (notamment en termes de volume horaire enseigné), il constitue un contrat d'engagement réel dans les forces armées, qui suppose d'être assujetti à l'état militaire et des missions et contraintes qui y sont liées. A l'heure actuelle, ce type de financement n'est pas formellement considéré comme un « financement pour la thèse », bien qu'il en possède la plupart des caractéristiques.

³³¹ Voir notamment les données présentes dans les chiffres clefs de l'état de l'Enseignement supérieur et de la Recherche en France sur la plateforme <https://publication.enseignementsup-recherche.gouv.fr>, plus particulièrement l'indicateur 38 consacrés aux doctorats et aux docteurs : « 38.5. Le financement des doctorants inscrits en première année de thèse (2009-10 à 2015-16) ». Pour l'année 2012-2013, sur 18 227 doctorants inscrits en première année dont la situation est connue, 12 405 sont indiqués comme bénéficiant d'un financement (contrat doctoral, convention industrielle de formation par la recherche, allocations d'une collectivité territoriale, etc.) hors situation de travail salariés. Autrement dit, 31,9 % des projets de thèse étaient non-financés.

³³² Ce n'est pas la seule unité de l'armée de l'air susceptible d'accueillir des doctorants au titre de sa mission.

2 – Mobilité géographique.

Dès le départ, cette recherche a impliqué une mobilité géographique importante. La communauté « cyber » et les différents acteurs du numérique ont très tôt orienté le terrain de cette recherche. Ne pouvant me déplacer dans tout le territoire français, les déplacements ont lieu tout d'abord entre Rennes et Paris où se réunissaient la plupart des événements de la communauté « cyber » en France (y compris en 2012). Si bien que lorsqu'il fallait rencontrer les différents acteurs, aller le faire à l'occasion de leur déplacement pour un évènement parisien était souvent plus simple. La création du « Pôle d'excellence cyber » initié notamment par le ministre de la défense en 2014 à la suite du « Pacte défense cyber », a renforcé cette dualité Paris/Rennes.

Du point de vue de la mobilité, le besoin s'est accru avec la délocalisation à Salon-de-Provence qui constitue le premier effet du recrutement de 2014. D'une part, car il fallait désormais pouvoir assurer la liaison entre la Bretagne et la Provence. D'autre part, le terrain avait lui-même évolué et nécessitait désormais plus de déplacements. Toutefois, la prise en charge de la mobilité a été en partie simplifiée grâce à l'aide du ministère des armées qui pourvoie au financement de quelques déplacements par an pour peu que ces derniers puissent être anticipés. Ceci aura permis de garder des liens avec l'université de terminer le terrain de la recherche, et participer à des conférences³³³.

3 – Les contraintes temporelles.

Il pourrait sembler étrange d'attribuer une valeur matérielle contraignante au temps dans le contexte de cette recherche. Tous les doctorants manquent ou finissent par manquer de temps à un moment donné. Si cette thèse n'échappe sans doute pas à la règle, elle a fait l'objet de contraintes de temps spécifiques. Tout d'abord, le choix d'une approche phénoménique plurale avec une approche statistique et un important dispositif d'observation participante a entraîné un temps de collecte et de traitement d'informations très important. Au-delà des contraintes évoquées sur la première période relative à l'activité salariée, le recrutement dans l'armée de l'air a entraîné un arrêt de fait d'un an entre septembre 2014 et septembre 2015. Cette année de césure a été partagée entre la fin de la préparation physique,

³³³ 25e Congrès mondial de science politique organisé en juillet 2018 à Brisbane par l'*International Political Science Association (IPSA)*.

la formation militaire, la récupération d'une blessure, la prise de fonction et le déménagement dans le sud de la France.

B – Difficultés rencontrées dans le travail de recherche

Nous avons déjà évoqué le questionnement épistémologique que constitue le fait d'aborder un objet politique mal identifié sous l'angle d'un ensemble théorique soumis à discussion. Si cette difficulté représente l'obstacle majeur que cette recherche s'emploie à contourner, d'autres difficultés ont pu survenir. Si le recrutement en cours de thèse a eu un grand impact sur les conditions matérielles de sa réalisation, elles auront eu assez peu d'impact sur ces difficultés qui sont inhérentes à la nature prétendument technique de l'objet et à ses représentations sociales. Il s'agit plus particulièrement trois questions : la légitimité de cette recherche, l'accès aux sources bibliographiques, et enfin l'exploitation des données collectées à partir du terrain.

1 – Légitimité d'objet et légitimité disciplinaire pour traiter l'objet.

Ce qui est perçu comme technique peut-il faire un objet scientifique en Science Politique ? Un doctorant en Science Politique peut-il aller jusqu'à « s'abaisser » à tenter de saisir un phénomène empreint de technique ? Que peut expliquer une thèse en théories des Relations Internationales des questions de sécurité informatique ? Cette question du rapport de l'objet à la technique fonctionne dans un double sens. Pour les sciences humaines, c'est souvent l'objet qui est décrié. Pour les sciences de l'ingénieur, c'est souvent la discipline qui n'est pas légitime à traiter de l'objet. Bien qu'il soit caricatural, d'établir ces deux catégories face à la complexité du monde scientifique, c'est souvent ainsi que l'on peut interpréter le questionnement de légitimité propre à l'objet. Au-delà de ces manifestations d'incompréhension, il faudra souligner que cette question de légitimité façonne aussi une grande partie des premiers débats de la communauté « cyber » en France. Le questionnement autour de la légitimité peut être étendu jusque dans le questionnement sur les aspects performatifs de l'enjeu politique de la sécurité de l'information. Plusieurs fois, sur le terrain de cette recherche, j'ai rencontré plusieurs émetteurs de discours (industriels, scientifiques...) qui n'avaient pas conscience de leur rôle actif dans la promotion et la légitimation d'un enjeu de sécurité.

2 – Les effets de l’actualité de l’objet « cyber » sur la production des résultats.

Si l’on travaille sur le cyberspace comme un discours, on est rapidement submergé par la quantité d’informations qu’il est possible de récolter. D’une semaine sur l’autre, il y a toujours une nouvelle définition plus actuelle, un nouvel événement, une nouvelle publication (le plus souvent à caractère non-scientifique), un nouveau logiciel, une nouvelle machine. Cela était d’autant plus vrai dans les années 2013, 2014 et 2015 où le phénomène a connu un nombre d’occurrence jamais atteint. Ces informations font parfois du chercheur sur l’objet, un adepte de la petite phrase et de la dernière sortie de tel ou tel responsable politique. Si ce travail de veille et d’interprétation est sans doute important à réaliser, il ne facilite pas la distance critique nécessaire à l’examen de l’objet. La solution mise en place réside dans la démarche abductive présentée plus avant. Se pose la question de la conformité de l’information récoltée ou plutôt de son degré de non-conformité duquel résulte une confiance ou une absence de confiance dans la fiabilité du résultat collecté. En effet, une information peut être fausse, incomplète, imprécise ou émise par une source douteuse. C’est d’autant plus vrai que le chercheur sur un objet comme le cyberspace se voit exposé à divers récits entrecoupés d’informations officielles, d’idées reçues et à d’indénombrables rumeurs. D’un point de vue empirique, la nature des informations ne présage pas de leur exactitude.

3 – L’exploitation des entretiens : sources d’informations et résultats exploitables

À travers les nombreuses personnes rencontrées et des entretiens réalisés, des documents accessibles, des événements scientifiques auxquels il a été possible de participer, voire d’organiser au cours de cette recherche, plusieurs types de résultats sont apparus. Ces résultats posent principalement la question de leur exploitabilité. Si l’observation participante fut un outil de collecte précieux au cours de cette recherche, on ne saurait en dire autant des entretiens réalisés de manière formelle. La plupart des entretiens formels réalisés dans le cadre de cette recherche ont été produits selon des stratégies exploratoires ou d’approfondissement. La fonction de l’entretien est ici assez classique en ce qu’il permettrait de comprendre le rapport au politique et d’analyser les valeurs, croyances et représentations des acteurs.

L’intérêt de l’entretien réside moins dans l’information elle-même que les processus de reconstruction de l’information par le discours. La personne interrogée devait donc jouir de la plus grande liberté possible pour orienter la discussion. C’est la raison pour laquelle

outre les questions « dites de talon », le protocole mis en place au travers du guide d’entretien comportait principalement une unique question de départ servant à définir le cadre de l’entretien. Pour la même raison, l’entretien n’a souvent pas pu être enregistré. La nature même de l’entretien impacte l’exploitabilité du résultat. Dans un premier temps, l’entretien a un effet de formalisation de la pensée que n’a pas autant la conversation menée dans le cadre d’une observation participante. Plus une personne est haut placée dans la hiérarchie d’une organisation scientifique, commerciale ou administrative ou encore est spécialiste d’un domaine, plus ses propos vont s’aligner sur le discours écrit de cette organisation ou son propre discours écrits (il n’y a donc pas besoin de l’entretien pour analyser le discours proprement dit, mais plutôt pour le déconstruire). Dans un second temps, tout propos qui s’éloigne de cet écrit peut également aboutir à des informations inexploitables à raison de leur confidentialité ou de leur sensibilité.

D’un point de vue théorique, il y a des informations « ouvertes » (disponibles à tous), « accessibles » (auxquelles un public restreint peut accéder), « inaccessibles » (qui relèvent à divers degrés d’un domaine confidentiel parce que couvert par une protection liée à la sécurité, aux secrets des affaires ou d’une instruction, ou plus simplement car elles relèvent de la vie privée). Ces informations peuvent par exemple être certains types de données personnelles³³⁴ qu’on ne peut pas employer comme on le souhaite, des éléments d’enquête ou des documents confidentiels provenant d’une entreprise ou de l’État. Pourquoi et comment telle information est-elle disponible ou non ? Cette question se rapproche de l’interrogation conduite sur ce qui peut être une source ou non du point de vue académique. Mais deux questions corolaires viennent ici interroger la recherche : l’hypothèse de la divulgation et le dilemme téléologique. Pour ce qui relève, de la première interrogation, la divulgation est un phénomène connu, voire devenu populaire notamment par le biais des « lanceurs d’alerte »³³⁵. Comme dans ce dernier cas la divulgation peut intervenir consciemment par opportunité mais aussi de manière inconsciente par mégarde. Cette première question vient déjà complexifier le travail autour de la source. A cela vient s’ajouter le questionnement téléologique. Ce dernier prend forme dans les Relations Internationales avec ce qui est souvent présenté comme la question du premier « grand débat » interparadigmatique qui a déjà été mentionné : Les études des Relations

³³⁴ Que nous comprendrons empiriquement de manière très restrictive, comme toute donnée susceptible de conduire à l’identification d’une personne physique ou morale...

³³⁵ Comme le sont devenues les figures d’Edward Snowden

Internationales servent-elles à expliquer les relations internationales telles qu'elles sont ou à les décrire telles qu'elles devraient être ? L'opportunité de la divulgation s'apprécie au sens de cette recherche à partir de cette question. Une action consciente de divulgation sert-elle l'explication ou la transformation de l'objet étudié ? Chaque chercheur pourra se positionner d'un point de vue téléologique voire déontologique face à ce questionnement.

Quel que soit le degré de confidentialité avéré d'une information collectée, son utilisation est-elle de nature à porter préjudice ? Les exemples en matière de sécurité de l'information sont assez évidents dans la mesure où il est possible d'acquérir une connaissance directe ou de déduire rapidement une grande partie des points faibles virtuels ou réels de n'importe quelle organisation. J'insiste sur ce dernier point. C'est le cas pour une entreprise, pour une université, ou pour les services de l'État. Le chercheur attentif pourrait par exemple découvrir que telle entreprise ou organisation utilisait jusqu'à quelques années des adresses mails fournies par un tiers avec un niveau de sécurité moindre rendant cette structure par exemple vulnérable aux opérations d'ingénierie sociale et d'espionnage. Autre exemple, le chercheur ou un tiers pourrait acquérir des données confidentielles d'une entreprise qualifiée d'opérateur d'importance vitale en utilisant le plus simple des moteurs de recherche y compris par hasard³³⁶. Un dernier exemple, davantage orienté sur les infrastructures, pourrait être la connaissance précise d'un local d'un opérateur téléphonique et fournisseur d'accès Internet (FAI) qui n'est absolument pas fermé à clef ou sécurisé et dans lequel tous les « câbles » sont accessibles. Si par civisme, le chercheur devra en informer l'organisation ou la personne concernée dans une démarche d'assistance, peut-il pour autant utiliser l'information comme un résultat de ses recherches ? Tout semble à croire qu'en la matière une précaution forte s'impose. Une liste des entretiens réalisés sera reproduite en annexe reprenant la fonction de personnes interrogées, les dates, les lieux, les durées et des informations sur l'organisation de l'entretien. Les noms des personnes interrogées ne seront pas reportés.

4 – L'accès aux sources bibliographiques et faiblesse des sources archivistiques.

L'accès aux sources bibliographiques a représenté l'un des grands enjeux de cette recherche. Il y a deux contraintes importantes à retenir : la langue étrangère (le plus souvent

³³⁶ Pour une affaire judiciaire concernant une soustraction frauduleuse de données par copie en utilisant Google, voir notamment l'arrêt de la chambre criminelle de la Cour de cassation du 20 mai 2015 n° 14-81.336, voir également le commentaire : AUFFRET Yves, "Le vol numérique en question", *Journal Spécial des Sociétés*, n°62/2015, 30 décembre 2015.

l'anglais) d'une majeure partie de la production scientifique à la fois sur les Relations Internationales mais également sur les aspects politiques de la sécurité de l'information ainsi que la faible disponibilité desdites publications dans les fonds en France. En dehors des manuels et des ouvrages généralistes lorsqu'ils sont présents, il n'existe qu'assez peu de références traitant de la sécurité de l'information et plus généralement d'Internet.

Ainsi, par exemple, la Bibliothèque nationale de France ne comporte qu'une quinzaine de références sur l'objet Internet qui ont semblé utiles à ce projet de recherche (dont la moitié en anglais). Sur les références de la bibliothèque de Science Po Paris, sur 51 références pertinentes *a priori* seulement 17 se trouvaient être en français. La bibliothèque universitaire des langues et civilisations de l'INALCO³³⁷ comportait en 2016 une quarantaine de références en anglais et en français (sans compter les références disponibles dans les nombreuses autres langues). Évidemment aucune de ces listes de références n'est exclusives et ce sont souvent les mêmes revues, ouvrages ou extraits qui sont référencés. Ces bibliothèques ont en commun qu'il faut souvent se déplacer à Paris afin de pouvoir y rechercher efficacement les informations utiles. Les déplacements à Paris depuis Rennes et la Provence ont permis un travail sur la bibliographie tout au long de la thèse de 2013 jusqu'en 2017.

Au quotidien, j'ai eu principalement accès à deux bibliothèques universitaires jusqu'en 2014 : la bibliothèque universitaire Droit, Economie, Gestion de l'université de Rennes 1 dont le projet a pu bénéficier principalement des ressources en lignes, et la bibliothèque de l'Institut du Droit Public et de la Science Politique, EA 4640. Le déménagement en Provence m'a privé d'un accès quotidien à une bibliothèque universitaire. Le centre de recherche de l'armée de l'air n'entretient pas de fond documentaire. Une médiathèque est présente sur le site de l'école de l'air, toutefois elle représente davantage un lieu de médiation culturelle qui met en relation un public cible (principalement les élèves-officiers recrutés sur concours externe) avec un contenu culturel très varié mais qui comporte malheureusement trop peu d'ouvrages académiques.

Au-delà d'un simple catalogue des publications, la disponibilité implique le caractère consultable du répertoire. De facto, de nombreuses publications sont souvent présentes dans d'autres bibliothèques voire présentes à l'étranger. Ce qui ne facilite pas leur consultation sur

³³⁷ Institut National des Langues et Civilisations Orientales.

place sans parler de leurs emprunts. Le caractère anglais de la production représente également un temps de traitement supplémentaire.

Sur le plan des archives disponibles, les sujets de la sécurité de l'information, de la cybersécurité, d'Internet, sont assez peu documentés du point de vue des Relations Internationales. Les premières tentatives de recherches dans les archives sur la thématique d'Internet s'est révélée assez pauvre en résultats. Il en va de même pour archives nationales qui en 2014 n'affichaient que 35 résultats sur le préfixe « cyber » dont aucun ne concernait directement l'objet de recherche. La décision d'écarter la construction d'un corpus de sources archivistiques sauf document particulier a été prise en janvier 2014. Lancé en mars 2017, le portail France Archives ne contenait aucune référence exploitable sur la cybersécurité et les références utiles concernant Internet ou le préfixe cyber sont des articles et des ouvrages qui se retrouvent déjà dans les réseaux des bibliothèques universitaires ou qui n'intéresse que peu les relations internationales en tant que thématique.

Ainsi après ce chapitre liminaire destiné à expliciter les éléments théoriques et pratiques de l'approche retenue dans ce travail de recherche, nous allons aborder la Première partie du manuscrit dédiée à l'étude du phénomène de l'utilisation du cyberespace et de ses termes dérivés.

Partie I – Du mot au discours, le tournant sécuritaire du cyberespace : Eviter les pièges de la recherche d'une définition unique.

« Je ne dispute jamais du nom, pourvu qu'on m'avertisse du sens qu'on lui donne. »

Blaise PASCAL³³⁸

³³⁸ A propos du terme « pouvoir prochain », Lettre n°1 du 23 janvier 1656, PASCAL Blaise, *Les Provinciales* (1656-1657), Gallimard, Folio classique, octobre 1987, 416 p.

Cette première partie du manuscrit est dédiée à l'analyse du phénomène linguistique que constitue le cyberespace et ses termes dérivés. Cette analyse qui opte pour la méthode plurale que nous avons décrite lors du chapitre liminaire sera divinisée en trois temps. Un premier temps est dédié à l'étude du rapport à la technique du phénomène analysé à travers la création du cyberespace dans la littérature de science-fiction.

Le chapitre 1 vise en particulier à introduire la notion de cyberespace tout autant qu'il critique la possibilité d'y trouver une définition à l'image de celle qu'on pourrait attendre d'une notion technique. Pour ce faire, le chapitre est articulé autours de trois idées que sont le pouvoir évocateur de la notion, son ambiguïté en tant que discours sur les technologies de l'information, et la méfiance ainsi rendue nécessaire à l'égard des tentatives de définition dans la littérature scientifique.

Le chapitre 2 de cette recherche étudie l'impact normatif des termes dérivés du cyberespace compris comme phénomène linguistique « cyber » à travers l'analyse logométrique de corpus composés de textes officiels (Journaux officiels français et européens, ainsi que le système de diffusion électronique des documents de l'ONU). Ces analyses sont comparées avec deux corpus médiatiques respectivement constitués à partir des bases de données de Factiva et de Google. L'ensemble de ces corpus est de langue française et inclus l'ensemble des références utiles entre le 1^{er} février 2001 et 31 octobre 2016. L'enjeu est ici de dégager certaines tendances dans l'ensemble de termes créés et de développer les bases d'analyse du contexte d'emploi des termes dérivés du cyberespace. Le travail de ce chapitre nous permettra de dégager les plus usités de l'emploi de ce discours et de commencer à faire le lien entre celui-ci et la sécurité de l'information.

Le chapitre 3 complétera cette première partie avec une réflexion générale sur les porteurs du discours centrée sur un dialogue entre la communauté discursive (qui emploie le langage « cyber ») et la communauté épistémique (qui produit de la connaissance sur la sécurité de l'information). Après une relecture du concept de communauté épistémique à l'aune de la notion de discours et une étude des frontières de la communauté, ce chapitre 3 fera le lien avec le terrain français en évoquant d'une part les sources anglo-saxonnes des concepts employés, l'émergence de la sécurité informatique avant que ne soient adopté lesdits concepts, la transformation de l'information en enjeux de sécurité nationale et le rôle particulier de la recherche académique dans la légitimation de cette transformation.

Chapitre 1 – Circulations et mutations du cyberespace : un objet hors de la technique ?

« Je connaissais par cœur toutes les puces du simulateur de Bobby ; il ressemblait à n'importe quel banal Ono-Sendaï VII, le « Cyberspace Sept », mais je l'avais reconstruit tant de fois qu'on aurait eu bien du mal à trouver un millimètre carré de circuit d'usine sur toutes ces plaques de silicium. »

William GIBSON³³⁹

L'extrait précité est issu des premières lignes de la nouvelle *Burning Chrome*, présentée pour la première fois à l'automne 1981 par son auteur William Gibson, alors âgé de 33 ans, lors d'un congrès de science-fiction à Denver. Il s'agit de la première occurrence du terme cyberespace qui est alors utilisé pour décrire un dispositif de simulation permettant d'accéder à un « non-espace » hallucinatoire dont la fonction est de permettre l'échange massif de données informatiques. En effet, si on doit rechercher l'existence du phénomène « cyber » dans l'histoire, ce dernier doit d'abord être envisagé sous l'angle de la lettre. Au commencement, le « cyber » est un effet de langage. En effet, le « cyberespace » ne résulte pas d'une invention dans le domaine de l'informatique, il s'agit avant tout d'une création littéraire ayant vu le jour dans le domaine de la science-fiction³⁴⁰.

Ce n'est qu'à raison du succès rencontré par le terme contenu dans l'œuvre de l'esprit, qu'il aura été possible d'assister à la récupération du terme pour décrire un ensemble de phénomènes complexes liés aux technologies de l'information. Cet état de fait implique d'entrée des contraintes qu'il est nécessaire de prendre en compte si on veut approcher le cyberespace et les phénomènes politiques que la notion recouvre. Ces contraintes sont de deux ordres : d'une part, des précautions liées à la relation étroite qu'entretient le sujet avec la

³³⁹ Premières lignes originales de la nouvelle *Burning Chrome*. Texte original publié pour la première fois en 1982 dans le magazine *Omni* : GIBSON William, « Burning Chrome », *Omni*, N° 46, juillet 1982 pp 72 - 77. Le texte a fait objet d'une nouvelle publication au sein d'un recueil à partir de 1986. La première version française de ce texte date de 1987, voir pour une version plus actuelle : GIBSON William, *Gravé sur chrome*, In. *Gravé sur chrome*, Paris, Éditions J'ai lu, mars 2006.

³⁴⁰ « Attention : fiction ne veut pas dire illusion. La fiction n'est pas hors de la réalité. Elle se réalise à tous moments. Nous l'appelons quelque fois utopie, bien obligés de reconnaître après un moment que cette utopie s'est réalisée et devient un élément de la réalité. Ou encore, on peut constater que malgré les réalités mises en place les germes d'utopie ne sont pas absents des réalisations ». SFEZ Lucien, « La technique comme fiction », *Revue européenne des sciences sociales*, XL-123, 2002.

fiction ; d'autre part, une nuance à apporter sur les tentations de récit a posteriori qui feraient du cyberespace un « pur » héritier de l'état de la technique et des mouvements de pensée qui l'ont précédé.

La pierre d'achoppement à laquelle se heurte systématiquement tout travail de recherche, ayant pour terrain ou objet le « cyberespace », est celui de la définition : qu'est-ce que cette notion est sensée recouvrir ? A-t'elle seulement un sens ? En effet, la question d'une possible définition du cyberespace est l'arlesienne des différentes études scientifiques ou techniques qui sont produites autour de cette thématique. C'est donc le meilleur point de départ pour répondre à la question « Comment comprendre le cyberespace ? » qui implique en premier lieu de mieux cerner ce terme³⁴¹.

Prenant le risque de répondre à la question d'une définition, les auteurs peuvent recourir à plusieurs approches. Il est possible de trouver des références à un ou plusieurs texte(s) de nature juridique ou doctrinale, des tentatives d'association à la technique³⁴², et enfin le renoncement dans l'affirmation de l'impossibilité d'une réelle définition complète à raison des multiples textes et de l'immensité du champ de la technique potentiellement concernés par la notion. Pourtant, le terme cyberespace est composé de deux racines qui renvoient à des concepts extrêmement précis : « espace » et « cybernétique ». Les approches du cyberespace fondent leur raisonnement sur une démarche chronologique ; laquelle inscrit l'émergence du cyberespace comme le produit la contraction du mot d'origine grecque « cybernétique » avec le mot d'origine latine « espace ». Ainsi, d'un point de vue diachronique, la plupart des auteurs aimeront évoquer l'étymologie du cyberespace. Le terme doit alors se comprendre comme le produit la contraction du mot d'origine grecque « cybernétique » avec le mot d'origine latine « espace ». Le cyberespace peut alors s'inscrire comme le fruit d'une

³⁴¹ Les présents développements utiliseront alternativement le « terme » et le « substantif » pour désigner les usages construits autour le racine « cyber » laquelle sera souvent désignée comme un « affixe » (préfixe, suffixe, interfixe, confixe) avec une entorse au sens linguistique puisqu'en étudiant ces usages nous intégrerons également les usages du « cyber » comme épithète. Les déformations propres à certains noms à usages commerciaux tels que « Cyb' Air » par exemple, s'ils ne seront pas forcément ignorés, seront exclus du périmètre des résultats de la recherche proprement dite.

³⁴² Association techniciste de nature idéologique qui réside au choix dans un consensus « mou » formé d'une liste non-limitative d'autres inventions ou concepts mis en relation avec le premier (Internet, Web, Matrice, Ordinateur, Câble, Smartphone, etc.) ou hélas parfois d'un aveu de méconnaissance ; le cyberespace est alors davantage un outil de promotion qu'un objet de recherche.

évolution sémantique prenant sa source dans l'Antiquité chez Platon³⁴³ pour émerger de nouveau dans la seconde moitié du XXème siècle.

La difficulté à définir le cyberespace va grandissante. Depuis une trentaine d'années, l'effervescence autour de ses différentes déclinaisons inscrit cette notion dans un phénomène de « néoténie », autrement dit de « reproduction à l'état larvaire » : les occurrences du terme croissent d'année en année, sans pour autant que cette quête d'une définition ne puisse réellement progresser. Deux causes cumulatives viennent affecter la progression du cyberespace d'une notion vers un concept ; et concourent à faire de la recherche d'une définition un véritable piège. Premièrement, le principe même d'une définition suppose la recherche des caractères ainsi que des limites de l'extension d'un concept ; deuxièmement, le reste du problème procède de l'oubli (volontaire ou pas) de la nature et des origines du terme. Si la plupart de la difficulté à définir le cyberespace procède de la recherche des limites du concept et de l'oubli de sa nature littéraire, c'est avant tout par l'effervescence qui mène l'évolution du terme vers ses dérivés que cette difficulté sera concrétisée. Relève ainsi de l'erreur d'appréciation, le fait de rejeter une posture critique en cherchant à penser et définir ontologiquement le cyberespace en tant que phénomène observable dans un espace « poppérien », résolument positiviste³⁴⁴.

Ne pouvant faire l'économie de l'hétérogénéité théorique à laquelle la notion de « cyber » conduit, il faudra inclure l'ensemble de ces évolutions sous un même cadre de départ qui permette son appropriation : Ici, la distinction entre le « concept polymorphe » et le « concept sténographique », empruntée à Jean-Claude Passeron³⁴⁵. Ces deux expressions doivent être comprises comme les deux adversaires de la « faisabilité » ou la délimitation stricte d'un lexique. Cette adversité réside dans la césure irréconciliable entre la langue de la théorie et la nécessité de l'observation.

³⁴³ κυβερνήτης (*kubernêtēs*), gouvernail. Notamment utilisé dans la réponse de Socrate à Adamante sur la question de l'utilité de philosophe à la cité et de pourquoi celui-ci finit par y apparaître comme pervers ou bizarre. Le gouvernail est employé ici comme la métaphore du pourvoir de gouverner, objet d'une lutte entre ceux qui ne savent point naviguer et qui prétendent que la navigation ne s'apprend pas, réfutant ici que la politique de la cité puisse faire l'objet d'une science. Extrait concerné : PLATON, *La République*, livre VI, Collection des universités de France, les Belles Lettres, 1932, § 488a - 490b

³⁴⁴ Cf. chapitre liminaire.

³⁴⁵ Plus précisément, à ses travaux de thèses inspirés de Ludwig Wittgenstein et de Karl Popper reproduits dans le chapitre 2 de l'ouvrage PASSERON Jean-Claude, précite, pp 31 à 56.

D'une part, le concept polymorphe décrit la situation dans laquelle un terme souffre la multiplicité des emplois descriptifs, source d'hétérogénéité, qui oblige le chercheur qui veut mobiliser un concept à la maîtrise de l'ensemble des définitions qui ont été produites et qui font le pouvoir théorique du concept. Ainsi, cette contrainte borne sa recherche à une maîtrise littérale des différentes sémantiques sans pouvoir conférer à son concept de réflexion générale ou de dimension critique. Le chercheur est ainsi contraint à un usage alternatif des termes et à une différenciation toujours plus spécialisée qui confine l'approche à celle des règles formelles, particulières ou communes à l'emploi des uns ou des autres. Derrière cette approche, prenant l'exemple de la « structure », Jean-Claude Passeron place l'idée que le concept polymorphe ne s'épuise pas dans une définition particulière, car il est toujours plus et autre chose que l'analyse qu'il permet de produire. Le cyberespace serait donc impossible à définir par le seul prisme des théories qui en font l'usage.

D'autre part, à l'opposé du concept polymorphe, trop théoriquement hétérogène, se trouve le « concept sténographique ». Celui-ci naît lorsque le chercheur rencontre au fil de son travail d'analyse une multiplication de termes *ad hoc* qui ne trouvent leur sens (unique) que dans le rapport au contexte et au matériel employé qui les constituent spécifiquement. Une apparente précision empirique qui mine la compréhension et résiste farouchement à toute tentative de conceptualisation qui établirait un lien entre ces différentes constructions. Plus généralement, cette approche peut avoir à rebours pour conséquence perverse de conduire à une analyse actualiste et volatile des termes. C'est une des tendances actuelles de la recherche sur le « cyber ». Ce qui est vrai aujourd'hui ne sera plus vrai demain et le nouveau concept doit religieusement remplacer l'ancien (ou l'ancienne acception du concept³⁴⁶). Le propre du travail autour d'un concept « cyber » est d'invoquer ce double obstacle à l'analyse de manière permanente : la pluralité des définitions de l'objet, tout comme la pluralité des termes qui en sont dérivés. Le cyberespace demeure un champ de la recherche en proie à une forme de néoténie³⁴⁷. Ainsi, il faudrait distinguer par une série de typologies linguistiques particulières

³⁴⁶ Un autre exemple d'artefact victime de cette tendance peut se trouver dans le drone, où l'UAV pour *Unmanned Aerial Vehicle* (Véhicule aérien non-embâqué) est « devenu » en 2011 le RPAS pour *Remotely Piloted Aircraft System* ou système d'aéronef piloté à distance. Voir l'ouvrage CReA, CESAA, *Les drones aériens : passé, présent et avenir : approche globale*, La Documentation Française, 2013, 706 p.

³⁴⁷ En référence à la biologie où la néoténie désigne la capacité de certains animaux à se reproduire à l'état larvaire.

ayant force de conceptualisation³⁴⁸, et dont il faudrait retracer pour chacune l'évolution et le contexte d'émergence, parfois jusqu'à l'absurde : la cyberdéfense et la cybersécurité, la cyberattaque et la cyberdéfense (comprise exclusivement dans le sens de cyberprotection), la cyberattaque et le cybercrime, la cyberrésilience et la cyberrésistance, ou encore la cyberblatte ou le cybercafard, insectes télécommandés, face au cyberpapillon, robot imitant la forme de l'insecte³⁴⁹... Se transformant sans cesse à la fois dans son sens et dans la forme, le cyberespace apparaît comme une notion qui circule entre littérature, science, commerce et politique autour de laquelle s'est cristallisée une communauté à caractère scientifique.

Afin de faire le point sur les différentes circulations du cyberespace qui ont favorisé la construction de cette figure qui servira de base au phénomène linguistique analysé. Ce chapitre se propose d'explorer le sens de cette figure à travers ses origines littéraires, des héritages dans lesquels elle s'inscrit, des points de recouvrement voire de confusion avec des notions voisines (Internet, Web) et de discuter son caractère prétendument technique.

Section 1 – Aux sources du pouvoir évocateur du cyberespace, invention, héritages et confusions.

Le point de départ de cette analyse sera fixé entre 1981 et 1984, autrement dit entre le moment de la première occurrence publique du terme et sa définition fictionnelle plus avancée qui l'a rendu populaire. Cette popularité aura vocation à dépasser l'œuvre initiale au grand étonnement de son créateur, par l'altération du sens premier du terme et sa déclinaison en de nombreux termes dérivés.

La présente section étudiera l'invention du cyberespace, les héritages sur lesquels la notion s'est construite dans les domaines scientifiques et culturels, et enfin quelques-unes des confusions qui entourent le terme.

³⁴⁸ Il faut voir dans les travaux issus de cette tendance, ce que Jean-Claude Passeron décrit comme une « virtualité féconde », autrement dit un travail de conceptualisation fondé sur l'hétéronomie des acceptations d'un terme qui parvient à garder un concept « lourd » à l'image de celui de « classe sociale » (op-cit. p.38 et 41).

³⁴⁹ Quo qu'il faille maintenant nuancer cette distinction étant donné que le sens de cyberpapillon a évolué entre 2001 et 2008 pour se rapprocher également de « l'insecte télécommandé » en lieu et place du « minirobot imitant la forme de l'insecte ». Cette première nuance établie il nous faudrait également la contrebalancer à l'aide d'une nouvelle itération « cyberabeille » qui reprend ce dernier sens en y ajoutant d'une part une dimension « autonome » et d'autre part, un rapport à la fonction de pollinisation assurée par l'insecte plutôt qu'à sa forme... Pour aller plus loin, voir notamment le programme de recherche de la DARPA sur les *HI-MENS* pour « *Hybrid Insect Micro-Electro-Mechanical Systems* ».

A – Invention et définition du terme cyberespace entre 1982 et 1984 : la littérature d’anticipation dystopique.

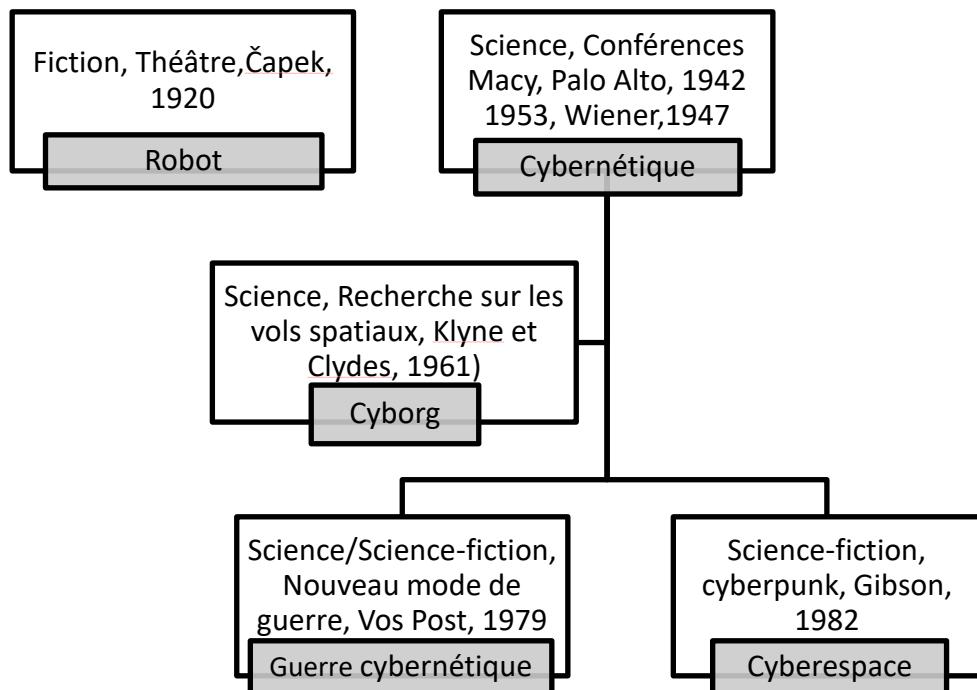


Figure 4 - Rappel sur l'origine des premiers termes voisins ou dérivés de la cybernétique.

Le mot cyberespace n'est pas issu des sciences ou de l'industrie informatique. Mais, à l'image du mot « robot »³⁵⁰, il est issu de la littérature. Les évènements qui amènent la création du terme « cyberespace » sont l'objet du documentaire *No Maps For These Territories*³⁵¹. C'est l'occasion pour l'auteur américain, William Gibson, de revenir sur les circonstances qui l'ont amené à créer ce terme. Cet évènement est à remettre dans le contexte de la naissance de la littérature dite « cyberpunk »³⁵², genre narratif construit autour de l'anticipation et la

³⁵⁰ Mot formé à partir de la racine slave « *работа* » (« *rabota* ») qui signifie « travail », attribué à l'auteur tchécoslovaque Karel Čapek, qui l'utilisa pour sa pièce de théâtre *R. U. R. (Rossum's Universal Robots)* [titre original : *Rossumovi univerzální roboti*], écrite en 1920 et jouée pour la première fois à Prague en 1921, puis à New York en 1922. ČAPEK Karel (trad. Jan RUBES), *R.U.R. Reson's Universal Robots*, Paris, Editions de La Différence, février 2011, 220 p.

³⁵¹ NEALE Mark, *No Maps For These Territories*, (4 novembre 2000), DVD, New Video Group, 25 novembre 2003. Pour une brève synthèse, voir également : LOHARD Audrey, « La genèse inattendue du cyberespace de William Gibson », *Quaderni : Cyberesp@ce & territoires*, Vol. 66, N°1, 2008 pp. 11-13.

³⁵² Terme également dû à William Gibson.

dystopie. Une œuvre cyberpunk dépeint un futur relativement sombre et proche, où les technologies sont souvent très avancées, mais en mettant en avant des personnages cyniques dans des univers violents et lugubres. Les thèmes majeurs et récurrents du genre sont le piratage (hacking), les multinationales possédant la puissance des États régaliens, ou l'intelligence artificielle.

Ces thèmes sont toutefois présents dans bien d'autres œuvres. L'œuvre de William Gibson a connu un succès commercial et critique³⁵³. Elle a par ailleurs inspiré de nombreuses autres œuvres³⁵⁴. Toutefois, il faut également souligner le succès du terme « cyberspace » en lui-même.

1 – Le cyberspace de William Gibson.

D'un point de vue littéraire, il est communément admis que le cyberpunk se termine quand il commence à se diffuser aux autres médias et à Hollywood (perdant ainsi le côté « punk »). Le mouvement qui commencerait au début des années 80 se terminerait à la fin de celles-ci ; qu'importe l'impact sur le cinéma, la télévision ou les arts graphiques ; la plupart des auteurs retournant finalement à la littérature policière dont ils étaient issus. C'est au cours de cet évènement que William Gibson fera la rencontre de l'auteur Bruce Sterling (lequel, en 1986, deviendra l'un des fondateurs du mouvement en proposant la première anthologie dite « cyberpunk », qui finit par incarner une forme de manifeste artistique³⁵⁵).

Lors de la présentation de la nouvelle, ce dernier complimente William Gibson sur ce nouveau terme. Plus avant dans le documentaire, l'auteur en explique la création ainsi :

« J'en étais arrivé à un point où il me fallait un mot à la mode. J'avais besoin de remplacer le vaisseau spatial et le holodeck par quelque chose qui serait un signe de changement technologique et qui me fournirait un moteur narratif et un territoire où la narration pourrait avoir lieu. [...] Tout ce que je savais

³⁵³ L'œuvre a été la première à remporter les trois littéraires majeurs de la science-fiction aux États-Unis : Le *Nebula Award* en 1984, le *Philip K. Dick Award* 1985 et le *Science Fiction Achievement Award* en 1985 (décerné par la *World Science Fiction Society*, devenu *Hugo Award* à partir de 1993) devançant à chaque fois l'œuvre d'auteurs plus confirmés comme Robert A. Heinlein (*Starship Troopers*, 1959), qui présentait son ouvrage *Job, a Comedy of Justice*.

³⁵⁴ Pour information, voici quelques exemples d'œuvres ayant puisé leur inspiration dans l'œuvre de Gibson: Robocop, Matrix, Ghost in the Shell, Akira, Johnny Mnemonic, ...

³⁵⁵ STERLING Bruce (ed.) *Mirrorshades: The Cyberpunk Anthology*, Arbor House, 1986, 320 p.

du mot cyberespace quand je l'ai inventé, c'est qu'il avait l'air d'être un mot à la mode efficace. Il était évocateur, mais essentiellement dénué de sens. [...] Il suggérait quelque chose, mais n'avait pas de vrai sens sémantique, même pour moi, quand je l'ai vu émerger sur la page. »³⁵⁶

Ainsi, du point de vue de son auteur, le « cyberespace » est moins le produit des racines grecque et latine qui le composent, que de la recherche d'un signe efficace et évocateur de progrès technique. La définition plus précise qu'il finira par donner au cyberespace en 1984, dans son ouvrage *Neuromancer*³⁵⁷, ne va pas contredire cette intention première. En effet, il y définit le cyberespace comme une « une hallucination consensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays » (la définition joue sur les aspects relatifs aux stupéfiants qui sont omniprésents dans l'œuvre) « par des enfants à qui des concepts mathématiques sont ainsi enseignés [...] Une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain ».³⁵⁸ Bien que le « cyberespace » de Gibson conserve une dimension pédagogique et sociale, la présence de métaphores décrivant cette dimension comme des « villes de lumière » ou des « nuages » et « constellations de données », dote ce cyberespace d'une dimension mystique qu'un seul opérateur perdu dans l'immensité de la population ne pourra jamais appréhender de manière complète. Il s'en dégage une raison pour laquelle le cyberespace ne peut pas être parfaitement bien défini : pour son créateur, il n'a pas à l'être en dehors de son pouvoir évocateur. Bien que lieu dans le récit, la dimension spatiale y est en fait étrangère par nature, et n'existe que pour permettre à l'opérateur de s'y projeter.

Plutôt qu'un espace proprement dit, il faut le réduire à l'idée du lieu, ou encore de théâtre pour des personnages. Ce cyberespace tourné vers la finalité n'a d'autre sens que celui qu'il évoque pour le lecteur. Le lien aux ordinateurs se révèle lui-même discutable ; l'auteur

³⁵⁶ Propos de William Gibson dans le documentaire, *No Maps For These Territories*, op-cit. Traduction également retenue et rapportée par LOHARD Audrey, « La genèse inattendue du cyberespace de William Gibson », op-cit. Les références aux vaisseaux spatiaux et à l'holodeck, font écho au film *Star Wars*, sorti en 1977 et à la série *Star Trek* diffusée originellement 8 septembre 1966 et 3 juin 1969. Positionné sur un autre domaine de la science-fiction (dit « space opera »), l'auteur entendait ici se démarquer dans une relation de concurrence face à ce genre narratif dominant à l'époque.

³⁵⁷ Edition originale : GIBSON William, *Neuromancer*, New-York, Ace books, juillet 1984, 271 p.

³⁵⁸ Définition originale tirée de *Neuromancer*, op-cit : « *Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding...* » Ibid.

n'a aucune connaissance technique en informatique. Le cyberespace ne peut pas être défini techniquement au moment de l'invention et de la définition du terme. Nous sommes entre 1981 et 1984, pour prendre en exemple l'un des ordinateurs contemporains de l'époque : l'ordinateur IBM PC/XT, ou modèle IBM 5160, commercialisé en 1983, qui affichait fièrement son processeur Intel 8088 cadencé entre 4.77 et 10 Mégahertz, une mémoire vive de base de 16 kilooctets, pour un disque dur de 5 Megaoctets.

Ce type de machine, même interconnectée à des millions d'autres³⁵⁹, ne peut raisonnablement pas devenir l'incarnation de la mémoire de l'humanité au travers d'un processus de réalité virtuelle combiné avec des stupéfiants, que des centaines de millions d'opérateurs utiliseraient, pour ne pas dire consommeraient, quotidiennement. Le « cyberespace » de Gibson n'existe pas. De plus, notre niveau actuel de développement ne permettrait pas de le restituer tel quel. Il faudrait sans doute rajouter : nous n'en prenons pas la direction. L'humanité procède même dans le sens contraire : inclure davantage les nouvelles technologies dans la vie quotidienne de l'opérateur, plutôt que de chercher à l'en extraire. L'un des exemples est l'idée d'augmentation de la réalité, qui repose sur un principe d'adjoindre la technologie à la vie quotidienne³⁶⁰. Cette idée de réalité augmentée s'oppose au cyberespace de Gibson qui décrit davantage le principe d'une réalité reconstituée à travers l'ordinateur, autrement dit une réalité virtuelle³⁶¹.

2 – Le phénomène « cyberespace » dans le langage.

La réussite de ce terme peut s'évaluer selon deux paramètres : l'extraction du terme de l'œuvre de fiction à laquelle il appartient *ab initio*, et la production de termes dérivés. La confiscation du cyberespace à son contexte d'origine doit se comprendre comme une évolution. Gabriel Tarde, penseur de la criminologie, à la fois rival d'Emile Durkheim et adversaire de la théorie de Cesare Lombroso, évoque l'évolution en ces termes : « l'Évolution

³⁵⁹ Sachant que la plupart de ces machines étaient déjà connectées en réseau local

³⁶⁰ Plus précisément, la réalité augmentée peut se définir comme une « interface entre des données informatiques et le monde réel ». Pour une approche plus technique des origines de ce concept, voir : AZUMA Ronald T., « A survey of Augmented reality », *Presence: Teleoperators and Virtual Environments* 6, 4, août 1997, pp 355-385.

³⁶¹ Concept popularisé par Howard Rheingold, enseignant à Berkeley, notamment dans ses ouvrages RHEINGOLD Howard, *Tools for Thought: The History and Future of Mind-expanding Technology*, MIT Press, 1985 - 359 p. , *Virtual reality*, Secker & Warburg, 1991 - 415 p. et RHEINGOLD Howard, *The Virtual Community: Homesteading on the Electronic Frontier* (1993), MIT Press, octobre 2000, 480 p.

n'est pas une voie, mais un réseau de voies anastomosées »³⁶². Il n'y a donc pas une évolution en ligne directe des idées, mais des échanges entre des processus qui suivent leurs logiques propres. Le cyberespace n'est pas passé de la fiction aux sciences puis au politique pour revenir vers nous après coup. Le cyberespace a été « coconstruit » tant par l'imaginaire, que par les champs scientifiques, industriels, politiques ou administratifs. « Construction collective, le cyberespace et ses avatars continuent d'être entretenus par des lecteurs [...] »³⁶³. Ce phénomène s'exerce notamment par le biais des termes dérivés du cyberespace à travers l'affixe « cyber- » qui concourent à faire de la notion un terme englobant pour de nombreux objets concrets.

Une étude de linguistique parue en 2001³⁶⁴, évalue la productivité du « cyber » comme celle d'un « affixe » qui finit par désigner « qualifier tout et n'importe quoi du moment que cela se rapporte à l'Internet et aux réseaux multimédias interactifs du futur de l'an 2000 »³⁶⁵. Du point de vue de cette étude, le « cyber- » peut ainsi renvoyer à la réalité virtuelle (« cybernaute » [...]), au contexte d'Internet ou des multimédias (« cyberdémocratie », « cyberdélinquance », « cyberterrorisme », « cybercafé » [...]), à la cybernétique, comprise en tant que branche de la robotique (« cyberblatte », « cyberpapillon », « cybermaison » [...]). Ce sont ainsi plus de 600 néologismes construits avec l'affixe « cyber- » qui sont identifiés au sein de l'étude.

Cette surabondance de dérivés du cyberespace est expliquée en partie par Thomas Michaud, dans son article « La dimension imaginaire de l'innovation : l'influence de la science-fiction sur la construction du cyberespace »³⁶⁶. Thomas Michaud décrit comment le

³⁶² L'auteur emploie cette métaphore dans la préface de son étude datée de 1891, *Les transformations du droit : étude sociologique*, alors qu'il introduit le concept d'imitation. L'anastomose est ici employée dans un sens dérivé inspirée de la signification médicale du terme qui décrit la connexion entre deux structures/ vaisseaux/organes, TARDE Gabriel, *Les transformations du droit. Étude sociologique*, (mai 1891), 2e édition, Paris, Berg International Éditeurs, 1994, 216 pp.

³⁶³ LOHARD Audrey, « La genèse inattendue du cyberespace de William Gibson », op-cit.

³⁶⁴ RAUS Rachèle, « Productivité de cyber et hyper dans le lexique français d'Internet », *La linguistique* 2/2001, Vol. 37, pp. 71-88

³⁶⁵ L'étude mobilise ici la définition familière du *Jargon français*, dictionnaire d'informatique. ROLAND, Trique (éd.) *Jargon français* [Site Internet]. Définition du « cyber » : <http://jargonf.org/wiki/cyber> [consultée le 1/09/2016].

³⁶⁶ MICHAUD Thomas, « La dimension imaginaire de l'innovation : l'influence de la science-fiction sur la construction du cyberespace », *Innovations*, n° 44, 2014/2, pp 213 - 233.

genre cyberpunk a nourri pendant les années de 1985 aux années 1990 une véritable dynamique accompagnant les recherches des ingénieurs et scientifiques dans le secteur des télécommunications, jusqu'à nourrir les investissements liés au point de finir par créer une bulle spéculative³⁶⁷ ³⁶⁸. Cette bulle, aussi connue sous le nom de bulle « Internet » affectant les valeurs technologiques qui finiront par imploser en mars 2000 du fait d'une exagération des investisseurs sur les perspectives à long terme et la véritable combustion du capital des sociétés affectées ; lesquelles dépensaient ce dernier bien trop vite pour pouvoir revenir à l'équilibre (les premières entreprises affectées par cet éclatement furent les opérateurs télécoms). Il n'en demeure pas moins que cet élan a profondément brouillé les frontières d'une notion qui n'en avait pas davantage besoin. Le principe reste le même que celui qui conduisait la démarche de William Gibson : un terme tourné vers le but qu'il s'était fixé. Ainsi, les récupérations du cyberspace ont procédé avec cette même logique. Le cyberspace n'est à la base qu'un terme évocateur efficace à la mode décrivant une réalité complexe en évolution autour des technologies de l'information. Néanmoins, quand bien même cette réflexion permet de mettre avant l'impossibilité de définir objectivement le cyberspace, elle ne permet pas d'en décrire le pouvoir évocateur de la notion à l'origine. Le seul succès de l'œuvre littéraire est sans doute l'un des éléments du faisceau d'indices qui peut expliquer l'impact du terme *a posteriori*. Pour comprendre le pouvoir évocateur du cyberspace *ab initio*, il faut examiner l'héritage sémantique à partir duquel il a été créé.

B – Le cyberspace comme revendication d'un héritage scientifique et culturel.

Dans son ouvrage *Les utopies posthumaines: contre-culture, cyberculture, culture du chaos*, Remi Sussan intègre cyberpunk et réalité virtuelle (Avec le « cyberchamanisme » et le « *New Edge* ») et les comprend comme étant la première partie d'une « cyberculture »,

³⁶⁷ Néanmoins, ce mouvement littéraire ne saurait être considéré comme le seul facteur d'émergence de cette bulle qui demeure avant tout le produit d'une industrie. Pour une étude économique sur l'impact du projet ARPANET dans la structuration du premier écosystème d'affaires autour des TIC fondé grâce à une rupture technologique portée par une communauté d'organisations où les grandes entreprises sont reléguées à la marge, voir notamment : BARBAROUX Pierre, « Innovation disruptive et naissance d'un écosystème : voyage aux origines de l'internet », *Revue d'économie industrielle*, 2/2014 (n° 146), p. 27-59.

³⁶⁸ Voir également, sur les acteurs privés et les technologies de l'information, l'ouvrage de la journaliste Dominique Nora. NORA Dominique (1995), *Les Conquérants du cybermonde*, Paris, Calmann-Lévy, avril 2014, 355 p.

entendue ici au sens de mouvement culturel contestataire³⁶⁹. Cette idée d’utopie est reprise par Benjamin Loveluck, dans l’ouvrage tiré de sa thèse, *Réseaux, libertés et contrôle*^{370 371}, et constituerait l’une des bases des discours de la libre circulation de l’information. Ce discours qui alimenterait alors un développement politique des technologies de l’information par le libéralisme informationnel tourné vers l’idée d’économie politique (comprise comme système général de régulation des échanges). Sans remettre en cause l’optique libérale de l’étude, dont la finalité réside dans l’implication du concept d’autorégulation à travers les flux de décentralisation, recentralisation et d’auto-institution des réseaux, l’idée de cyberespace selon Gibson n’est jamais univoque³⁷². S’il est tout à fait possible de considérer l’œuvre du point de vue de sa critique du capitalisme, il ne faut pas négliger que la dimension apocalyptique du récit est également une source de l’ensemble des discours sécuritaires et catastrophistes liés à cette même thématique.

Les propos de William Gibson que nous avons rapportés incitent à ne pas accorder plus d’importance au sens qu’il voulait donner à son œuvre, qu’à la réception de celle-ci. Même si l’auteur évoque la création du cyberespace comme un heureux accident, il est facile de cerner quelles ont pu être ses influences. La racine « espace » ne permet pas de comprendre en tant que tel le pouvoir évocateur du cyberespace en dehors de sa seule dimension territoriale attachée à un récit. Comprendre le cyberespace ne peut donc exclure l’appréhension de son autre racine : « cybernétique ». Dans sa définition du cyberespace, excluant la réalité virtuelle, Daniel Ventre rappelle que cette racine « cyber » est avant tout un préfixe d’origine grecque qui confère aujourd’hui à « tout ce qui a un lien avec les ordinateurs, l’informatique, les réseaux ou Internet »³⁷³. Néanmoins l’étude de Rachel Raus identifie trois « champs lexicaux

³⁶⁹ Il inscrit cette culture dans la filiation du « mouvement hippie ». Il envisage ainsi ces deux mouvements auxquels il adjoint la « culture du chaos » comme autant d’utopies posthumaines. SUSSAN Remi, *Les utopies posthumaines: contre-culture, cyberspace, culture du chaos*, Omniscience, coll. Les essais, 2005, 287 p.

³⁷⁰ LOVELUCK Benjamin op-cit.

³⁷¹ Pour un regard géopolitique sur cette notion d’utopie du cyberespace, voir la première partie des travaux de thèses d’Alix Desforges : DESFORGES Alix, *Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l’exemple de la France*, soutenue le 27 août 2018 à l’Institut français de Géopolitique, Université Paris 8 Vincennes/Saint-Denis, sous la direction de Frédéric Douzet, 398 p

³⁷² AUFFRET, Yves, « L’interdépendance des sciences sociales et de la fiction dans l’évolution des objets sociaux : L’exemple du cyberespace. » intervention, lors du colloque « Fiction et sciences sociales - Bonnes et mauvaises fréquentations », organisé par le CESSP (Paris 1 Panthéon Sorbonne / EHESS) au Conservatoire National des Arts et Métiers (Paris) les 25 et 26 septembre 2014.

³⁷³ VENTRE Daniel , *Cyberespace et acteurs du cyberconflit*. Hermès Publishing. Paris, 2011, p. 13

» auxquels l'affixe cyber peut faire référence : la « réalité virtuelle », « Internet et les médias », ainsi que la « robotique »³⁷⁴. Depuis l'année 2001, se pose ainsi la question de l'appauvrissement du lexique attaché au préfixe « cyber ». De fait, les problématiques liées aux « drones » et à la robotique sont aujourd'hui traitées à part des problématiques liées au « cyberspace », au mépris de l'héritage scientifique du terme (A). Il en va de même pour les problématiques « d'augmentation humaine » qui ne sont pas incluses sous le terme « cyborg », quand bien même c'est ce premier néologisme qui a sans doute inspiré l'auteur (B).

1 – L'héritage de la pensée systémique et le mouvement cybernétique.

Au-delà de ses racines platoniciennes, le terme cybernétique a notamment été utilisé dans un sens identique par Ampère afin de décrire l'art de gouverner³⁷⁵. Il faudra attendre le début du XXème siècle, pour que ce mot se teinte d'une dimension « technique ». Dans son entretien controversé à *Der Spiegel* réalisé en 1966³⁷⁶, Martin Heidegger, décrit la cybernétique comme « *das andere Denke* » (« l'autre pensée ») issue des sciences, prenant la place de la Philosophie à une heure où celle-ci a rempli son rôle et se dissout dans les « *Einzenwissenschaften* » (« sciences individuelles ») que sont la psychologie, la logique et la science politique³⁷⁷. Néanmoins, une telle acception se révèle caricaturale dans ce qu'elle dit de l'état de la technique.

Du point de vue de l'histoire des sciences, la cybernétique incarne un courant pluridisciplinaire actif entre 1942 et 1953, forgé autour des « Conférences Macy »³⁷⁸. Au cours de la première de ces conférences, Arturo Rosenblueth présente les bases de l'article fondateur de la cybernétique, « Behavior, Purpose and Teleology », qu'il publiera avec Norbert Wiener

³⁷⁴ RAUS Rachèle, 2001, op-cit.

³⁷⁵ AMPERE André-Marie, *Essai sur la philosophie des sciences ou Exposition analytique d'une classification naturelle de toutes les connaissances humaines*, Paris, Bachelier, 1834, 654 p.

³⁷⁶ Entretien réalisé en 1966 et publié après la mort de Martin Heidegger dans *Der Spiegel* 31 mai 1976 (pp. 193 - 219), pour une analyse de l'entretien, voir HACHMEITER Lutz, *Heideggers Testament. Der Philosoph, der Spiegel und die SS*, Propyläen, Berlin, 2014, 368 p.

³⁷⁷ *Der Spiegel*, 31 mai 1976, op-cit. p. 212.

³⁷⁸ La Josiah Macy, Jr. foundation, appelé aussi « fondation Macy », est un organisme américain né en 1930, qui œuvre dans le domaine de la santé et de l'éducation. A l'initiative du neuropsychiatre et mathématicien Warren McCulloch, la fondation organise en 1942 une conférence sur le thème de l'« inhibition cérébrale » qui se consacre principalement à l'étude des phénomènes hypnotiques. Cette première conférence fut l'événement déclencheur du courant.

et Julian Bigelow³⁷⁹. C'est seulement à la suite de cette intervention que Warren McCulloch, créateur de la fondation voyant les liens entre ces travaux et ceux qu'il a entrepris avec Walter Pitts³⁸⁰ et propose le lancement d'un cycle de conférences qui deviendra les fameuses « Conférences Macy », soit une dizaine de rencontres entre 1942 et 1953. Le courant connaît une sorte de schisme entre une « première » et une « seconde » cybernétique. C'est d'abord un moyen de connaissance, une discipline cognitive, qui étudie l'information comme objet au sens de la physique et son importance dans les interactions systémiques. Cela se ressent déjà dans la définition qu'en donne Norbert Wiener : « L'information fournie par une série de messages est une mesure d'organisation³⁸¹ ». L'information est ici distincte de l'entropie. La notion majeure de ce courant demeure le « Feedback ». Wiener va l'expliquer quant à lui par le mécanisme de la boite noire. Le principe est simple : La boite noire est un élément relié à d'autres et dont le mécanisme est insondable. L'enjeu va être le contrôle du flux d'information (ici synonyme de l'information efficacement transmise). Le *feedback* ou le retour sur information va être nécessaire pour pouvoir caractériser des logiques d'autorégulation, donc des systèmes. C'est une analyse des systèmes par voie de conséquences : Le système n'est pas forcément l'objet de l'étude de cette première tendance.

Alors que la « première cybernétique » étudie comment les systèmes maintiennent l'homéostasie par des mécanismes d'autorégulation, la « deuxième cybernétique » du psychiatre William Ross Ashby et des biologistes Humberto Maturana et Francisco Varela étudie quant à elle la question de savoir : « comment les systèmes évoluent et créent des nouvelles structures ? » (On parlera ainsi de morphogenèse). Cette étude des systèmes éloignés de leur point d'équilibre se rapproche des travaux sur les structures dissipatives. On se trouve alors dans une logique systémique avant l'heure³⁸². Les situations extrêmes recèlent

³⁷⁹ ROSENBLUETH Arturo, WIENER Norbert et BIGELOW Julian, « Behavior, Purpose and Teleology », In. *Philosophy of Science*, 10: 18-24, 1958, Version française, « Comportement, intention et télologie », In. *Les Etudes Philosophiques*, 2, 1961, pp. 147-56.

³⁸⁰ Notamment MCCULLOCH Warren, et PITTS Walter, « A logical calculus of the ideas immanent in nervous activity », *Bulletin of Mathematical Biophysics*, University of Chicago Press, 1943.

³⁸¹ WIENER Norbert, *Cybernétique et société, l'usage humain des êtres humains*, Paris, UGE, coll. « 10/18 », 1954, 248 p.

³⁸² Il est important de souligner que cette vision de la systémique tient davantage du « fonctionnalisme » que du « structuralisme ». La cybernétique se construit d'abord comme la mesure de l'effet d'information d'un système abstrait et non pas sur les mécanismes internes de celui-ci. Cet état de fait apparemment anodin permet de neutraliser le système à considérer et d'appliquer les théories défendues par ce mouvement à tout type de « système » : d'une machine à l'être humain.

la possibilité de créer une forme de nouvelle structure. On voit ici la possibilité de recréer du vivant, de l'organiser là où il n'y avait plus que du chaos. Le pas sera franchi davantage avec l'inclusion de l'observateur dans l'analyse par Heinz van Foerster³⁸³. Lequel rappellera simplement : « Pour écrire une théorie du cerveau, il faut un cerveau ». Cette cybernétique dite de « deuxième ordre » visera à l'élaboration d'une méthode de description « universelle » commune aux différents champs de la science. D'autres travaux, ont le mérite de souligner les apports et impacts de ces travaux sur le champ scientifique de l'époque (théorie de l'information, psychologie sociale, thermodynamique...)³⁸⁴. Il peut sembler paradoxal de retrouver dans ce courant à la fois l'origine scientifique des théories de l'information puis d'Internet autant que la source du rattachement entre cybernétique et technique. Ce serait oublier que science et fiction, sont ici deux champs parallèles. Même si le fait générateur du cyberespace se situe côté littérature, la genèse du cyberespace s'explique par un long processus d'échanges entre des processus qui suivent leurs logiques propres. Pour la compréhension de la genèse du « cyberespace », il faut en retenir une association des concepts issus de ces travaux comme le système, l'espace et l'interaction avec les thèmes de la transcendance et du progrès³⁸⁵ qui ont permis leur diffusion bien au-delà du seul champ scientifique. Toutefois, c'est bien ce nouveau sens donné au terme « cybernétique » qui permettra ensuite son appropriation dans le domaine littéraire à partir des années 60 (2).

2 – L'héritage des premières appropriations de la cybernétique : le « cyborg » et la « guerre cybernétique ».

William Gibson n'a pas donné son sens technique à la cybernétique, il n'a pas non plus été le premier à vouloir s'en servir dans un néologisme. L'une des premières appropriations du terme réside dans une recherche du lien entre humain et machine ; l'un des premiers dérivés

³⁸³ ANDREWSKY Evelyne et DELORME Robert, *Seconde cybernétique et complexité - Rencontres avec Heinz von Foerster*, coll. Philosophie des sciences et techniques, L'Harmattan, Paris, juin 2006, 168 p.

³⁸⁴ Voir par exemple : SEGAL Jérôme, *Le Zéro et le Un : histoire de la notion scientifique d'information au 20e siècle*, Syllepse, 2003, 890 p. ; FAUCHEUX Michel, *Norbert Wiener, le Golem et la cybernétique*, Paris, Editions du Sandre, Paris, 2008, 188 p.

³⁸⁵ Au niveau de la mise en relation de ce courant scientifique avec les idées de progrès et de transcendance, voir notamment : LAFONTAINE Cécile, *L'Empire cybernétique. Des machines à penser à la pensée machine*, Paris, Seuil, 2004, 240 p. ; ainsi que les travaux de thèse de Nicolas Ledevèdec : LEDEVEDEC Nicolas, *La société de l'amélioration : du renversement de la perfectibilité humaine, du l'humanisme des lumières à l'humain augmenté*, thèse de science politique sous la direction de Céline LAFONTAINE et Jean BAUDOUIN, Université de Montréal / Université de Rennes 1, soutenue en septembre 2013 (non publiée).

de « cybernétique » est le terme « cyborg ». Souvent compris comme un terme de science-fiction décrivant un humain ou une créature dont certains membres ont été « remplacés » par des machines, le cyborg est en réalité popularisé par des travaux en neurosciences et en pharmacologie sur le vol spatial dans les années 60³⁸⁶. L’« organisme cybernétique » effectue une légère altération du sens du mot cybernétique pour désigner non pas un organisme qui effectue un échange efficace dans le but de réaliser une action³⁸⁷, mais à un humain amélioré pour survivre aux conditions de vie d’un environnement extra-atmosphérique. Pour l’anecdote, Norbert Wiener dans son ouvrage *cybernétique et société*³⁸⁸, décrit le concept d’échange efficace en recourant à la figure de la machine dans l’éventualité où celle-ci serait capable de prolonger les processus d’autorégulation du système humain³⁸⁹ : une sorte de réponse à la phrase qu’il écrivait plus tôt « Nous sommes des naufragés sur une planète vouée à la mort »³⁹⁰.

Plus tard, le terme « cyborg » aura également une seconde vie scientifique notamment par son utilisation en tant que concept politique dans les travaux de Donna Haraway³⁹¹. Néanmoins, son usage dans la littérature de genre des années 60 et 70 aura fourni l’un des outils permettant à Gibson de forger le néologisme cyberespace (tout en utilisant des

³⁸⁶ CLYNES Manfred et KLINE Nathan S. « Drugs, Space, and Cybernetics: Evolution to Cyborgs » In FLAHERTY Bernard, E. (éd.) *Psychopharmacological Aspects of Space Flight*, New York: Columbia University Press, 1961 pp 345–371 ; voir également sur l’idée de « symbiose homme-machine », LICKLIDER Joseph Carl Robnett, « Man-Computer Symbiosis » *IRE Transactions on Human Factors in Electronics*, Mars 1960, p.4.

³⁸⁷ WIENER Norbert, op-cit.

³⁸⁸ Op-cit., voir notamment le chapitre 5 de l’ouvrage, notamment les passages relatifs à la description des organismes et à l’individualité humaine comparée à la machine. Celle-ci est uniquement employée ici à titre de métaphore, que l’auteur juge lui-même comme relevant du « fantastique ».

³⁸⁹ Contrairement à l’idée reçue, Norbert Wiener n’y emploie pas le terme robot, probablement par crainte d’une connotation trop fictionnelle. Le terme robot existe déjà depuis les années 20 (cf. supra). Mais, l’auteur de science-fiction Isaac Asimov a décrit ses 3 lois de la robotique depuis 1942 : ASIMOV Isaac, « Runaround », *Analog Science Fiction and Fact*, Mars 1942.

³⁹⁰ WIENER Norbert, op-cit. p. 49.

³⁹¹ Le cyborg y fait figure de concept politique permettant d’aborder le féminisme d’un point de vue critique, on retient la qualification de « cyberféminisme ». Voir notamment : HARAWAY Donna, « A Cyborg Manifesto : Science, Technology, and Socialist-feminism in 80’s », *Socialist Review* 15, no. 2, 1985 ainsi que *Simians, Cyborgs and Women : The Reinvention of Nature*. New York, Routledge, 1991, 312 p. Pour une analyse, voir notamment LEDEVEDEC Nicolas, *La société de l’amélioration [...]*, op-cit, pp 208 - 220. Voir aussi : GARDEY Delphine, « Au cœur à corps avec le Manifeste Cyborg de Donna Haraway », *Esprit*, mars-avril 2009, pp. 208-217.

augmentations cybernétiques dans ces mêmes récits)³⁹². Le terme « cybernétique » a également été associé en tant qu'adjectif à l'idée de conflit avec la notion de « guerre cybernétique » décrite dans très un court article en 1979 par Jonathan Vos Post comme un scénario possible de la troisième guerre mondiale : une guerre où les technologies informatiques se diffuserait à l'ensemble des systèmes d'armes³⁹³. Ainsi au-delà du constat que la « guerre cybernétique »³⁹⁴ existe avant le « cyberespace », il nous faut souligner que William Gibson dispose ainsi à la fois d'un terme connoté « à la mode » ainsi que d'un modèle déjà mis en place par les travaux scientifiques et les œuvres de fiction de l'époque³⁹⁵.

Cet héritage double forme les racines desquelles le cyberespace tire son pouvoir évocateur, que sa définition volontairement vague vient renforcer. De là, procède également la difficulté d'en produire une définition parfaitement claire. De plus, l'absence de celle-ci qui fonde notre présente approche doit également faire face à un ensemble de confusions liées à cet environnement complexe dont les technologies de l'information et leurs enjeux ne sont qu'un aspect, mais un aspect essentiel.

C – Cyberespace et définition(s) technique(s) : Déconstruire les idées reçues.

« Je vais tenter de fournir une esquisse préliminaire du cyberespace. Mais tout d'abord, la question suivante : quel rapport entre « cyberespace » et « réalité virtuelle », « visualisation de données », « interfaces utilisateur graphiques », « réseaux », « multimédia », « hypergraphie », etc. mots clés pour les développements récents dans la technologie informatique ?

³⁹² *Les androides rêvent-ils de moutons électriques* de Philip K. Dick (1966) est une inspiration évidente de l'œuvre de Gibson, mais aussi le roman *Cyborg* de Martin Caidin (1972) (œuvre qui donnera le téléfilm puis la série à succès *l'Homme qui valait 3 milliards* diffusée à partir de 1973).

³⁹³ Jonathan Vos Post est à la fois scientifique, professeur au *California Institute of Technology* (« Caltech ») et écrivain de science-fiction, VOS POST Jonathan, « Cybernecitic War », *Omni*, mai 1979, pp 44-50.

³⁹⁴ A ne pas confondre avec la cyberguerre, proposé dans la même revue par Owen Davies en 1987. DAVIES Owen, « Robotic Warriors Clash in Cyberwars, » *Omni*, vol. 9, n°4, janvier 1987.

³⁹⁵ Notre propos, choisit ici de se focaliser sur les éléments proches ayant un lien avec le terme cyberespace en omettant volontairement les apports plus anciens issus de l'imaginaire ou les références plus lointaines parfois assumées, comme les « Maschine Mensch » du film *Metropolis* du cinéaste Fritz Lang réalisé en 1927, ou encore plus loin : le système de transports des sons, dans *La Nouvelle Atlantide* de Francis Bacon écrit en 1627 : Cette même machine qui permet à des scientifiques collecteurs d'informations d'envoyer des sons sur de longues distances en se moquant de la topologie des paysages.... Si on regarde l'histoire le cyberespace s'inscrit en filigrane depuis des siècles. Il n'est pas nécessaire de remonter si loin pour dégager pleinement ce que peut être le cyberespace. Toutefois ces précurseurs : La littérature d'anticipation et l'histoire des sciences et des idées, présentent l'intérêt de mettre en lumière un processus d'émergence de longue durée.

La réponse : le cyberespace se rapporte à tous. Plus que cela, dans un certain sens, le "cyberespace" les inclut tous et une grande partie du travail effectué sous leurs rubriques. En fait, j'affirmerais que le cyberespace est un projet et qu'en tant que concept, il a la capacité de rassembler ces projets disparates en un seul objectif - pour les concentrer sur un objectif commun, pour ainsi dire.

Cela dit, mes efforts ici ne suffiront probablement pas à donner une image claire et utile de cette cible pour tous. Et c'est comme il se doit. »³⁹⁶

La plupart du temps, définir le cyberespace ne va pas plus loin qu'un inventaire technique des éléments constitutifs de celui-ci, qui ne font d'ailleurs que brouiller les quelques frontières de la notion. Cette dimension technique se traduit également par l'idée d'interconnexion mondiale, à la fois considérée comme territoire et comme structure. La définition ne s'attarde que peu sur l'aspect informationnel. C'est la traduction d'une vision dite « occidentale » ou « euro-américaine » fondée sur la technique.

1 – Confusion(s) sur le cyberespace : la « Toile » et les « sphères » de l'information.

Le pouvoir évocateur du cyberespace, que nous identifions comme l'une des causes de son succès, doit être mis en parallèle de la relative permissivité du terme. En effet, si nous avons évoqué la prolifération des dérivées à travers l'affixe « cyber- ». La recherche du sens du cyberespace a également conduit divers acteurs à attribuer une véritable légion d'épithètes à ce terme. Dans l'un de ses ouvrages, *Cyberespace et acteurs du cyberconflit* publié en 2010, Daniel Ventre s'essaye à décortiquer une partie de ces variations parmi les plus importantes³⁹⁷. Le seul constat est celui d'une relative perdition dans la question des termes à employer. Soit ce questionnement relève d'une recherche réelle de la nature du cyberespace et dans sa situation par rapport aux autres espaces ; soit ce questionnement procède d'une déformation du terme cyberespace par le discours qui peut prendre deux formes : d'une part, la substitution tacite du mot espace au profit d'un autre ce qui entraîne au choix un paradigme de la distance

³⁹⁶ BENEDIKT Michael, « Cyberspace: Some Proposals. » In. BENEDIKT Michael (ed.), *Cyberspace: First Steps*. Cambridge, The MIT Press, 1994, p. 122

³⁹⁷ VENTRE Daniel, *Cyberespace et acteurs du cyberconflit*, op-cit. pp 13 - 102. Ce serait prématuré et redondant de toutes les relever à ce stade de l'analyse ; néanmoins on peut constater que sur la seule idée « espace » on trouve déjà de tout : Du classique « espace d'affrontements » à un « espace à conquérir » en passant par des pléonasmes qui s'ignorent : « espace d'interactions », « espace créé par l'homme » ou encore un « espace qui a ses propres règles ». En vérité, ces variations n'apportent pas grand-chose au développement de la notion. Sur les aspects métaphoriques des analogies réalisées, voir également l'article : BETZ David J. et STEVENS Tim. « Analogical Reasoning and Cyber Security. » *Security Dialogue*, vol. 44, no. 2, 2013, pp. 147–164.

(Domaine, environnement ou dimension de puissance) et un paradigme de l'action (Capacité, processus ou défi vis-à-vis du pouvoir).

D'autre part, elle peut procéder d'une adjonction d'épithètes dont on peut se demander la pertinence. Néanmoins, ce véritable foisonnement relève davantage d'un apport à l'étude du cyberespace que d'un véritable obstacle ; il en dit long sur l'« effet de mode » qui poursuit le terme. En revanche, un réel problème réside dans la confusion qui règne dans le lexique d'Internet et de ses usages. En effet, dans une acception plus moderne, le cyberespace devient *de facto* synonyme d'Internet dans le langage courant. Ce même Internet se confond, lui-même, avec le *World Wide Web*. Cette assimilation au lexique d'Internet entraîne deux conséquences : d'une part, le cyberespace de Gibson réduit à Internet ne peut pas exister ; d'autre part, les travaux de recherche liés à l'information comme enjeu politique se réduisent à aborder la dimension « Internet » sans prendre en compte l'ensemble des enjeux transversaux liés à l'objet³⁹⁸. Il convient donc d'expliciter les distinctions à opérer entre ces termes ; bien qu'il faudra parfois surmonter cette différence afin d'en pouvoir mener à bien l'analyse.

La compréhension du cyberespace est dès lors entamée : d'un point de vue caricatural, il faut le considérer en tant que en tant que « métaphore » littéraire ouverte. A la différence, Internet et le « Web » et sont des inventions spécifiques et tout à fait concrètes... Par ailleurs, la création du cyberespace nous indique que celui-ci est marqueur d'une transformation sociétale par l'outil informatique. C'est la raison pour laquelle il convient de préciser ce que le cyberespace n'est pas. C'est à dire, d'une part, qu'il n'est ni Internet, ni le Word Wide Web, d'autre part, qu'il n'est assimilable ni à l'idée « numérique », ni à l'électronique, ni à la connaissance, ni au concept d'« information », par la brève comparaison avec quelques exemples associés parmi différentes utilisations conjointe du concept de « Sphère » et de celui d'information.

³⁹⁸ De plus, il est possible d'identifier des travaux « d'intérêt cyber » qui n'exploitent pourtant pas cette notion ainsi que des travaux estampillés « cyber » qui se servent de ce dernier comme une étiquette pour valoriser leur travail sur un objet différent.

2 – Cyberespace et objet « Internet » : les origines d’Internet et du « Web ».

« Internet » », cette création humaine est l’un des derniers fruits de deux phénomènes de longues dates qui se nourrissent entre eux : l’accroissement de la communication, qui pousse à la dématérialisation, et cette dernière qui banalise le premier³⁹⁹. Contrairement au cyberespace, Internet est une invention technique à l’histoire complexe. Il se comprend comme le seul réseau de portée « mondiale » interconnectant théoriquement l’ensemble des ordinateurs⁴⁰⁰. Une interconnexion de moindre ampleur est donc un simple « réseau » ; Internet est alors compris comme « le réseau des réseaux. L’agrégation des réseaux couplée à l’apparition des usages commerciaux d’Internet le popularise et en transforme les usages qui étaient auparavant réservés à un public restreint.

Le fait le plus marquant de la naissance d’Internet est la création du protocole TCP/IP en 1974⁴⁰¹. Avant la publication de ce protocole, il a été possible d’assister à une première phase de recherche qui commence avec l’invention du premier « modem »⁴⁰² en 1958. Cette première phase de recherche aboutira à la création de quatre réseaux : ARPANET de la *Defense Advanced Research Projects Agency* (DARPA) des États-Unis (projet lancé en 1969, première démonstration en 1972), le projet de réseau Cyclades (lancé en 1971), le réseau X.25 (débuté en 1971 également). Les réseaux *Unix to Unix Copy Protocol* (UUCP), quant à eux, apparaîtront un peu plus tard à partir de 1976. A partir de 1982, ARPANET se convertira protocole TCP/IP, et l’adopte officiellement à partir du 1er janvier 1983. Durant la même année, la partie d’ARPANET appartenant aux forces armées des États-Unis fut séparée du reste du réseau et devint le MILNET (*Military Network*). Avec la collaboration de la *National Science Foundation* (NSF), à partir de 1984, un premier réseau spécifiquement conçu pour le protocole TCP/IP voit le jour. Ce réseau finira par intégrer ARPANET ainsi que la dorsale

³⁹⁹ BERSINI Hugues, SPINETTE-ROSE Marie-Paule, SPINETTE-ROSE Robert, et VAN ZEEBROECK Nicolas, *Les fondements de l’informatique : du bit au cloud*, (2008) 3ème édition, Paris, Vuibert, septembre 2014, 404 p. (Cf. ici le chapitre 5 de l’ouvrage : Les réseaux, et surtout le passage relatif au contexte pp 195-202)

⁴⁰⁰ En principe n’importe quelle interconnexion entre des ordinateurs peut se voir qualifiée d’internet ; d’où des occurrences du pluriel : « les internets », même s’il semble qu’il s’agisse d’une dénomination impropre.

⁴⁰¹ Le protocole est formulé en 1973, néanmoins la publication de celui-ci s’effectue en 1974 : CERF Vinton. G. et KAHN Robert E., « A protocol for packet network interconnection », *IEEE Trans. Comm. Tech.* , vol. COM-22, V 5, mai 1974, pp. 627-641.

⁴⁰² Contraction de « modulateur-démodulateur », le dispositif transforme les données analogiques d’une ligne téléphonique en données numériques, et opère à l’inverse pour renvoyer les données.

NSFNET (créeée en 1986) dans un réseau étendu que l'on nommera « Internet » ; le protocole TCP/IP permettra par ailleurs une agrégation de l'ensemble des réseaux (comme ceux de type X.25), ce qui facilitera l'exportation des technologies Internet dans une grande partie du monde entre 1982 et 1990. C'est également à cette période que commenceront les débats sur la privatisation et la « fracture numérique » entre les différents États. Le *World Wide Web*, proprement dit, commencera seulement à apparaître à partir de la proposition de Tim Berners-Lee, du Conseil européen pour la recherche nucléaire (CERN) à Genève, le 13 mars 1989⁴⁰³.

L'année 1993 voit les premiers abonnements grand public, tandis que les œuvres marquantes de cette « seconde culture » Internet qualifiées du terme de « pionniers » verront seulement le jour entre 1993 et 1997^{404 405}. Pour Manuel Castells, cette histoire peut être théorisées comme la rencontre de quatre cultures particulières que sont celles des chercheurs (naissance technologique), des *hackers* (culture du partage), des communautés virtuelles (production culturelle et sociabilité virtuelle) et des entrepreneurs (expansion d'Internet)⁴⁰⁶.

3 – Discontinuité entre cyberespace et information : Infosphère et sphère informationnelle.

Une notion assez proche de celle du cyberespace est celle d'infosphère (qui comprend elle-aussi quelques termes dérivés sans connaître le même succès). En 1980, Alvin Toffler conceptualise l'infosphère dans son ouvrage *La troisième vague*⁴⁰⁷, ouvrage au cœur des

⁴⁰³ BERNES-LEE, Tim, *Information Management: A Proposal*, CERN, mars 1989.

⁴⁰⁴ Mentionnons ici, les travaux d'Howard Rheingold sur les communautés virtuelles : RHEINGOLD Howard, *The Virtual Community: Homesteading on the Electronic Frontier*, Addison-Wesley, 1993, 325 p. (voir également l'édition augmentée : MIT Press, 23 oct. 2000, 480 p.), les travaux sur les « netizens » : HAUBEN Ronda et HAUBEN Micheal, *Netizens : on the history and impact of Usenet and the Internet*, Wiley-IEEE Computer Society Press, mai 1997, 361 p. Pour l'anecdote, la même année était publiée la *Déclaration d'indépendance du cyberespace*, de John Perry Barlow (initialement une critique de la réforme des télécommunications aux États-Unis en 1996).

⁴⁰⁵ Pour plus d'information sur la naissance d'Internet et du Web, notamment sur les travaux des chercheurs liés à ces inventions, voir: SERRES Alexandre, *l'émergence d'ARPANET. Exploration du processus d'émergence d'une infrastructure informationnelle. Description des trajectoires des acteurs et actants, des filières et des réseaux constitutifs de la naissance d'ARPANET. Problèmes critiques et épistémologiques posés par l'histoire des innovations*, Thèse de doctorat en science de l'information et de la communication, Université Rennes 2, soutenue en octobre 2000, 590 p. Pour le cas français : *La France en réseaux: Tome 1, La rencontre des télécommunications et de l'informatique (1960-1980)*, Vol. 1, Collection Économie et prospective numériques, CIGREF, 2012, 380 p. Pour une vision critique et la mise en relation de ces événements avec leur dimension sociale, voir surtout ZETLAOUI Tiphaine (dir.), *Histoire(s) de l'Internet*, L'Harmattan, avril 2015, 226 p.

⁴⁰⁶ CASTELLS Manuel, *La Galaxie Internet*, Paris, Fayard, 2002, 365 p.

⁴⁰⁷ TOFFLER Alvin, *La troisième vague*, Paris, Folio, coll. Essais, 1980, 635 p.

théories des vagues de développement qu'il formule avec son épouse Heidi Toffler entre 1971 et 1994. Ces vagues (agraire, industrielle et « de la connaissance » ou infosphère) sont présentées comme de vastes mouvements sociaux superposés et venant s'enrichir mutuellement imprimant au passage l'histoire de l'humanité depuis les premiers temps du néolithique (soit au démarrage de l'agriculture). Dans ce contexte, l'infosphère s'attache à la vague de la connaissance qu'elle recouvre. C'est-à-dire l'adjonction de nouvelles strates de communication au système social, lesquelles relèguent la seconde vague industrielle (assimilée à la poste, le téléphone puis le « mass-média ») à quelque chose de « primitif ».

Si elle ne revendique pas la création du terme infosphère, cette œuvre et les autres œuvres des théories des vagues de développement ont permis son application à une dimension prospective qui viendront nourrir d'autres œuvres scientifiques (comme la littérature de science-fiction). Ces théories ont notamment permis l'émergence des théories de la société de l'information. En 1989, l'auteur de science-fiction Dan Simmons va employer le mot infosphère dans sa saga *Hypérion*, pour décrire une évolution possible d'Internet : un réseau parallèle enfanté de l'immanence de milliards de réseaux interconnectés aboutissant au final à l'émergence ésotérique d'une intelligence artificielle transcendant non seulement l'humain, mais la vie elle-même, accomplissant à sa place une forme de transcendance qui l'amènera vers une forme de divinité⁴⁰⁸. A la fin des années 90, Luciano Floridi, important théoricien de la philosophie de l'information prendra lui-même ce concept pour définir « l'espace sémantique constitué de la totalité des documents, des agents et de leurs opérations »⁴⁰⁹.

Different du sens que l'on peut lui attribuer dans les différentes approches des Relations Internationales, le terme d'« agents » fait référence à tout système capable d'interagir avec un document de façon autonome, comme par exemple une personne, une organisation ou un robot logiciel sur le Web. Un agent dans l'infosphère est un type spécial de document, capable d'interagir de manière autonome. Enfin, par « opérations », on doit comprendre tout type d'action, d'interaction et de transformation qui peut être effectué par un

⁴⁰⁸ D'autres œuvres de fiction plus récentes feront usage de ce terme dans un sens un peu différent. En particulier, la série d'animation *Futurama* dans laquelle l'infosphère est une encyclopédie universelle parlante en forme de sphère.

⁴⁰⁹ FLORIDI Luciano, *Internet: un exposé pour comprendre, un essai pour réfléchir*, Paris, Flammarion, 1998, 127 p. ; FLORIDI Luciano, *Philosophy and Computing: An Introduction*. Routledge, Londres / New York, 1999, 256p.

agent et à laquelle peut être soumis un document. Le concept, dans un sens différent de celui de la fiction, trouve donc à s'appliquer dans le domaine de l'information en général. Finalement, le terme infosphère décrit une représentation différente du cyberespace⁴¹⁰. C'est toutefois l'approche discursive qui a été retenue en Russie au travers du concept de « sphère informationnelle » qui peut se traduire de la stratégie russe par « sphère de l'activité humaine qui a pour objet la construction, création, transformation, transmission, l'usage est le stockage des informations ayant un effet perceptible sur la conscience personnelle et sociétale, la réalité ou les infrastructures de l'information »⁴¹¹.

Les liens du cyberespace à la fiction s'atténuent afin de le lier à une évolution contemporaine des technologies de l'information. Ce lien est devenu si fort que l'on ne peut plus réellement circonscrire les limites de ce cyberespace du point de vue du langage courant. Néanmoins, de telles confusions ne doivent pas apparaître comme une remise en cause du terme cyberespace lui-même, qu'il importe l'apparent degré de différence avec son usage premier. En effet, la consécration du cyberespace comme discours n'est qu'un prolongement d'une part, de l'absence de « sens » voulue par son créateur, et d'autre part, de son contexte d'émergence. Ce caractère construit du cyberespace préexiste à l'ensemble des démarches tendant à l'analyse de ce dernier. Ces démarches ne pourront ainsi être valides sans s'interroger de manière critique sur le but de l'utilisation de ce marqueur et des dérivées plutôt que sur un éventuel sens concret d'une abstraction volontairement incertaine.

Section 2 – Le cyberespace comme discours ambigu sur les technologies de l'information.

L'introduction aux travaux de Marcel Mauss réalisée par Nathan Schlanger dans *Techniques, technologie et civilisation*⁴¹², réaffirme que l'appréhension et la définition de ce

⁴¹⁰ Le terme s'appuie sur les notions de « noosphère », ou sphère de la pensée humaine et « biosphère » issue de la pensée de Vladimir Vernadsky et Pierre Teilhard de Chardin. VERNADSKY Vladimir I., « The Biosphere and the Noosphere », *American Scientist*, (janvier) 1945, 33(1), p. 1-12. ; VERNADSKY Vladimir I., *Biosphera (The Biosphere)*, Scientific Chemico-Technical Publishing: Leningrad, 1926, 200p. La noosphère conçue comme le milieu des représentations humaines est l'une des nombreuses notions à avoir été reprise pour parler de la stratégie cyber américaine dans une étude de la Rand corporation, ARQUILLA John et RONFELDT David, *The Emergence of Noopolitik: Toward An American Information Strategy*, RAND Corporation, Santa Monica, 1999, 89 p.

⁴¹¹ Pour une analyse en détail, voir notamment : HARREL Yannick, *La cyberstratégie russe*, Nuvis, 2013, 245 p.

⁴¹² SCHLANGER Nathan, « Une technologie engagée : Marcel Mauss et l'étude des techniques en sciences sociales » in. *Marcel Mauss, Techniques, technologie et civilisation*, Paris, PUF, coll. Quadrige, septembre 2012, pp 17-134

que l'on considère comme les techniques amènent vers plusieurs questions que sont le travail, la matérialité, l'appropriation de la nature, la production ; et que l'ensemble de ces idées implique des références croisées aux sciences, à l'économie, à l'environnement, à la culture, à la civilisation. Nathan Schlanger postule ainsi qu'une bonne conception de la technique, ou des techniques, est celle qui permet également d'inclure la dimension collective de celle(s)-ci, mais que les frontières entre technique et technologie sont brouillées. Il identifie alors deux débats sémantiques opposés.

Le premier débat consiste à considérer la technique comme l'objet avec les pratiques instrumentales afférentes, tandis que la technologie doit se comprendre comme le discours qui en traite et la discipline qui sert à décrire l'objet concerné⁴¹³. L'autre débat impacte davantage le sens et la réception de la technique. Dans cet autre paradigme, la technologie acquiert une double signification moderne et positive valorisée par rapport à la technique (artisanale, traditionnelle, indigène ou primitive). La technologie désigne ainsi des « phénomènes modernes, sophistiqués, industriels, des systèmes complexes »⁴¹⁴ ; lesquels peuvent être regardés positivement (progrès) ou négativement (aliénation de l'humain). Désigner certains phénomènes comme des techniques ou des technologies implique alors deux jugements sur ceux-ci sous le prisme de la modernité⁴¹⁵ : d'une part, le degré de cette modernité du phénomène ; d'autre part, une évaluation sur son caractère « positif » ou « négatif » pour l'humain.

Afin de comprendre cette ambiguïté, il est nécessaire de l'étudier sur trois aspects : l'ambigüité du lien entre technique et société, celle des technologies de l'information, et enfin celle qui existe entre le discours sur la technique et la société à laquelle nous confronterons l'idée de cyberespace.

⁴¹³ Ibid, p. 19

⁴¹⁴ Ibid, p. 21

⁴¹⁵ Afin d'illustrer ces différences sémantiques, l'auteur prend comme exemples le couple « techniques du corps » contre « technologies du corps », et le couple « techniques de pêche » contre « technologies de pêche » qu'il dépeint comme relevant « même intuitivement » de deux réalités très différentes. Nathan Schlanger se refuse à fixer un usage particulier de la technique ou de la technologie, à l'image de Mauss dont il caractérise des emplois irréguliers des deux termes, mais souligne la fragilité épistémologique de la notion de technique.

A – Penser les rapports entre la technique et la société.

Il n'a pas fallu attendre le XXème siècle pour que la technique se voit attribuée un caractère ambigu. L'ambivalence du sens de la technique est aussi ancienne que l'origine du terme bien avant la consécration du terme moderne au XVIIème siècle. Le mythe de Prométhée tel que nous le relate le *Protagoras* de Platon évoque déjà la technique de manière duale. Ainsi, le feu et l'art⁴¹⁶ sont dérobés à Héphaïstos et Athéna et utilisés par le titan pour combler les erreurs de son frère Épiméthée qui a pourvu les animaux de toutes les qualités pour survivre sans en laisser à l'humain. Cependant, bien que Zeus punisse Prométhée pour ce crime envers les dieux, il est également contraint de faire de nouveaux cadeaux à l'humain pour assurer sa sauvegarde. C'est ainsi que justice et pudeur sont offertes à l'être humain pour le prémunir de sa propre destruction par la technique. Ce nouveau don est également envisagé comme la source du sens politique et de l'opinion de chaque individu. La technique est donc une source d'émancipation pour la race humaine, mais aussi un danger potentiel pouvant anéantir l'espèce s'il n'est pas « limité » par le politique. Lorsqu'Aristote a décrit la technique, ce n'était que pour l'inscrire dans une vision particulière de l'intellect construite autour de l'idée de vertu. Dans ce système de pensée, la *technè* désigne une forme de disposition à la production dont le principe premier est lié au sujet de manière similaire à l'action (*praxis*) et non comme une forme de production « naturelle » (*poiesis*)⁴¹⁷.

Si détailler davantage l'étymologie de la technique⁴¹⁸, ou son origine en tant que concept semble a priori peu pertinent pour parler de technologies de l'information, leurs évocations permettent de positionner la technique en tant que l'un des piliers d'une conception matérialiste du monde. C'est-à-dire, un ensemble de visions qui considèrent ontologiquement que la réalité est le seul fait de l'humain et de ses interactions. Il en va de même pour

⁴¹⁶ Entendue au sens de l'« habileté artiste », la créativité chez Platon mais que Marcel Mauss en héritier de l'anthropologie assimile alors au « sens de l'outil » ou *knife sense*, composante de la technique.

⁴¹⁷ Pour une synthèse, voir notamment : DENAT Céline, *Aristote*, Paris, Ellipses, 2010, 180 p. ainsi que : COULOUBARITIS Lambros « Chapitre 6. L'aristotélisme », In. *Aux origines de la philosophie européenne*, Bruxelles, De Boeck Supérieur, « Le Point philosophique », 2003 (4^e éd.), p. 387-563. Pour une synthèse comparée de Xenophon aux stoïciens, voir aussi : PARRY Richard, « *Episteme and Techne* », In. Collectif, *The Stanford Encyclopedia of Philosophy*, The Metaphysics Research Lab, Standford, septembre 2014.

⁴¹⁸ Pour une synthèse, voir notamment : DENAT Céline, *Aristote*, Paris, Ellipses, 2010, 180 p. ainsi que : COULOUBARITIS Lambros « Chapitre 6. L'aristotélisme », In. *Aux origines de la philosophie européenne*, Bruxelles, De Boeck Supérieur, « Le Point philosophique », 2003 (4^e éd.), p. 387-563. Pour une synthèse comparée de Xenophon aux stoïciens, voir aussi : PARRY Richard, « *Episteme and Techne* », In. Collectif, *The Stanford Encyclopedia of Philosophy*, The Metaphysics Research Lab, Standford, septembre 2014.

l'information. Si la technique vient au côté du travail et de la production⁴¹⁹, l'information, quant-à-elle, ne saurait ainsi apparaître sans la matière et l'énergie⁴²⁰. Ces héritages apparaissent comme la source d'un problème épistémologique particulier qui fait qu'il n'est possible d'atteindre la technique qu'à travers l'artefact. Cela entraîne un détour de la pensée qui implique un examen critique du poids de l'artefact sur la production scientifique qui traite de la technologie. Dans la présente section, cette critique sera développée dans le rapport de la technique à la société, à l'information et au discours. D'un point de vue philosophique, la technique doit s'envisager de manière connexe à celle de l'art, de la science ou encore du travail. Qu'est que la technique ? Selon Heidegger, deux définitions solidaires l'une de l'autre peuvent être communément identifiées : son caractère de moyen finalisé, et son caractère propre aux êtres humains qui fondent une conception instrumentale et anthropologique de la technique. Cherchant à dépasser cette première définition, Heidegger aboutit par un commentaire d'Aristote et de Platon au « dévoilement » et à la distinction entre « production » (associé à la technique) et « pro-vocation » (associée à la technique moderne) qui lui permet de construire une vision ambivalente de la technique⁴²¹. Cette vision s'inscrit d'un point de vue métaphysique comme la description du rapport de l'humain à la nature qui rejoint la question de la vérité de l'être. L'ambivalence de la technique peut se comprendre dans le passage à la modernité et le transfert d'un dévoilement de l'être au savoir-faire par l'oubli du premier et dont l'aboutissement correspond à la *Machenschaft* (« Empire du faire »). Le danger de la technique moderne réside ainsi dans l'appropriation de l'humain par la technique elle-même. Menace pour le « dévoilement », ce danger ne peut être définitivement écarté quelques soient les efforts entrepris.

⁴¹⁹ HABERMAS Jürgen (1968), *La technique et la science comme « idéologie »*, trad. et préface par LADMIRAL Jean-René , Paris, Gallimard, 1973, 213 p.

⁴²⁰ Pour une histoire de l'information entendue comme concept matérialiste et une forme « d'illusion idéaliste » autour de l'information, voir notamment : CHAZAL Gérard, « Chapitre 15. La notion d'information et le matérialisme », *Matériaux philosophiques et scientifiques pour un matérialisme contemporain. Volume 1*, Paris, Editions Matériologiques, « Sciences & philosophie », 2013 (1), pp. 455-479.

⁴²¹ « La technique n'est pas la même chose que l'essence de la technique. [...] Nous demeurons partout enchaînés à la technique et privés de liberté, que nous l'affirmions avec passion ou que nous la niions pareillement. Quand cependant nous considérons la technique comme quelque chose de neutre, c'est alors que nous lui sommes livrés de la pire façon : car cette conception, qui jouit aujourd'hui d'une faveur toute particulière, nous rend complètement aveugles en face de l'essence de la technique. »⁴²¹ Extrait de la conférence « La question de la technique » de 1953, publié dans le recueil HEIDEGGER Martin (1954), « La question de la technique », dans Essais et conférences, Paris, Gallimard, coll. « Tel », n° 52, 1980, pp. 9 - 48.

Cet exemple d'approche est révélateur du lien particulier qui unit les concepts de la technique au travail et à la production... Cet héritage sera généralement marqué par une conception instrumentale de la technique au mépris de son lien au savoir⁴²². Cette question renvoie pour partie aux postures intellectuelles face à la technique.

1 – Les postures intellectuelles face à la technique : système, causalités et réseau.

Selon une typologie de Madeleine Akrich formulée en 1994⁴²³, il est possible de classer les différentes approches de la technique en trois grandes catégories pluridisciplinaires : les approches fondées sur une vision de la technique comme un système autonome, les approches centrées sur la construction des sociétés par la technique et des techniques par la société, en enfin une catégorie d'approche conjointe où la technique est indissociable de la société. Autrement dit, où « la technique n'apparaît plus que comme une modalité particulière d'association durable des humains entre eux et avec des entités non humaines »⁴²⁴. Ces principaux modèles constituent autant de réponses à la question de comment dépasser un clivage entre société et technique. Bien que cette typologie rejette toute prétention à l'exhaustivité, elle offre une grille de lecture pertinente des approches savantes de la technique qui dépasse les variables « optimistes » ou « pessimistes » et donc la seule question de l'artefact pour s'intéresser aux rôles de la technique qui déterminent voire constituent la place de ce dernier. « [...] pour comprendre ce que sont et ce que font les techniques, il est nécessaire de les déconstruire et d'analyser leur constitution. Autrement dit, le processus d'innovation et les controverses auxquelles il donne lieu mettent en jeu non seulement la définition des techniques, mais, corrélativement et de façon indissociable, celle de la société dans laquelle s'inséreront les techniques. »^{425 426} Au-delà des limites inhérentes

⁴²² GUCHET Xavier, « Pensée technique et philosophie transcendante », *Archives de Philosophie*, 1/2003 (Tome 66), p. 119-144.

⁴²³ AKRICH Madeleine, « 5. Comment sortir de la dichotomie technique/société. Présentation des diverses sociologies de la technique », In LATOUR Bruno et LEMONNIER Pierre (dir.), *De la préhistoire aux missiles balistiques. L'intelligence sociale des techniques*. La Découverte, 1994, pp. 103-131. Voir aussi : AKRICH Madeleine, « Comment décrire des objets techniques », *Techniques et Culture*, n°9, 1987, pp. 49-64.

⁴²⁴ Ibid.p. 107.

⁴²⁵ Ibid p. 106.

⁴²⁶ Pour une mise en application de cette typologie autour de la construction sociale de la technique à partir des exemples de l'automatisation des machines-outils, du guidage des missiles nucléaires et des tentatives d'apporter la preuve mathématique de la correction des systèmes informatiques de sécurité, voir MACKENZIE Donald, « 6. Ordinateurs et missiles de croisières. La sociologie des techniques contemporaines », In. LATOUR et LEMONNIER, op-cit., 1994, pp. 132-148.

à cette typologie qui se veut non-exhaustive et orientée dans la recontextualisation théorique d'une sociologie des techniques, elle a l'avantage d'identifier les grands types d'articulation entre technique et société. Ces articulations sont intéressantes à connaître du fait qu'elles conditionnent une partie du travail scientifique sur le cyberespace compris en tant notion par nature technique.

Dire que la technique est un système plus ou moins autonome revient à lui reconnaître la capacité d'autodétermination à l'image du système cybernétique. Dans cette vision la technique est ainsi capable d'administrer son développement par des mécanismes internes qui représentent une contrainte autonome par rapport à l'extérieur de la technique (le monde social par exemple). Il y a donc une normativité technique distincte de la normativité sociale. L'auteure distingue deux types d'approches systémiques : celles fondées sur une autodétermination « faible » ou « partielle » et celles fondées sur une autodétermination « forte ». La variation entre le fort et le faible s'exprime à travers la place accordée à l'environnement de la technique dans sa détermination⁴²⁷. Dans un cas comme dans l'autre, les règles internes déterminent un champ des possibles dans lequel la technique évolue. Néanmoins, dans un système à autodétermination forte, la technique n'est pas analysée dans une problématique d'émergence, mais au contraire pour dénoncer une emprise de celle-ci sur son environnement. Dès lors, on peut observer un renversement dans la recherche de la causalité. C'est une pensée de la domination où la technique est perçue de manière pessimiste. Si l'auteure mobilise principalement Marcuse⁴²⁸ et Ellul⁴²⁹, cette perspective pourrait également s'étendre aux conceptions de Jurgen Habermas et de la différence qu'il établit entre la rationalité instrumentale et l'interaction médiatisée par des symboles pour décrire la domination de la technique et son emprise sur le politique⁴³⁰. Entre autodétermination forte et

⁴²⁷ Sur cette double causalité interne et externe, Madeleine Akrich mobilise notamment l'histoire et la philosophie avec les exemples de Bertrand Gille, Jacques Laffite et Gilbert Simondon. Cf. GILLE Bertrand (dir.), *Histoire des techniques*, Paris, Gallimard, La pléiade, 1978, 1680 p. ; LAFFITE Jacques, *Réflexions sur la science des machines*, Paris, Vrin, 1972, 136 p. ; et, dans une édition plus récente, SIMONDON Gilbert (1958), *Du mode d'existence des objets techniques*, Aubier, 2012, 367 p.

⁴²⁸ Elle fait principalement référence à MARCUSE Herbert (1964), *L'Homme unidimensionnel*, Paris, Editions de Minuit, 1968, 281 p.

⁴²⁹ Voir dans l'édition la plus récente : ELLUL Jacques (1977), *Le système technicien*, Paris, Calmann-Lévy, 2012, 396 p.

⁴³⁰ HABERMAS Jürgen, *La technique et la science comme « idéologie »*, Gallimard, 1990, 213 p.

faible, l'auteure situe les travaux de Langdon Winner⁴³¹. Ces travaux se distinguent des précédents dans la mesure où la technique y a plusieurs modalités d'action en fonction de sa flexibilité. D'une part, il y a des techniques « intrinsèquement politiques » (le nucléaire) qui reposent sur un État organisé et suivent un modèle similaire à une autodétermination forte, et les techniques flexibles (solaire) qui peuvent adopter diverses formes d'autodétermination faible. Quels que soient les modèles, leur niveau d'autodétermination et leur point de départ variés, la plupart de ces modèles ont des caractéristiques communes qui forgent une ontologie particulière de la technique. Tout d'abord, l'individu y tient une place secondaire, y compris lorsqu'il est l'inventeur de la technique en question, et ne pèse pas beaucoup dans l'émergence d'une technique par rapport aux autres conditions du modèle (qui varient en fonction de celui-ci)⁴³². Ces auteurs font de la technique un système, ce qui implique qu'il n'y a pas de différence entre les phénomènes « macro » et « micro » du point de vue de la technique dans ce qu'elle est et ce qu'elle fait. De plus, en tant que système interrelié, la technique s'autodétermine dans une mise en cohérence des éléments qu'elle lie. Et enfin, les rapports entre science et technique, ainsi que les besoins qui président à l'émergence des techniques sont totalement transparents pour les auteurs⁴³³.

Dans une deuxième catégorie de modèles, la technique et la société sont des ensembles qui se construisent mutuellement. Seront distingués les modèles globaux où la technique est une production globale forgée par la société, des modèles de causalité locale qui ont pour particularité de rejeter les causes générales permettant d'expliquer la direction et la forme prise par le développement des technologies. Dans le premier cas, la technique peut être regardée comme une propriété de l'environnement humain (social, biologique). Dans le second cas, la technique peut amener des transformations sociales (innovation).

Concernant les modèles globaux, la pensée particulière de trois auteurs est mobilisée. la technique selon André Leroi-Gourhan qui comme s'inscrit dans le prolongement de

⁴³¹ Il est particulièrement fait référence à la version de l'article « Do Artifacts Have Politics? » republiée dans l'ouvrage collectif *The Social Shaping of Technology*, dirigé par Donald A. MacKenzie et Judy Wajcman en 1985. Nous ferons ici référence à la première publication WINNER Langdon « Do Artifacts Have Politics? », *Daedalus*, Vol. 109, No. 1, Hiver 1980, pp. 121 - 136.

⁴³² AKRICH Madeleine, op-cit, p. 111.

⁴³³ Ibid.

l'évolution naturelle⁴³⁴; la technique comme prolongement de l'organisation politique chez Lewis Mumford⁴³⁵; et la technique en tant que dynamique socio-économique dans la réception des écrits de Marx⁴³⁶. En dépit de la très grande hétérogénéité des penseurs associés à cette catégorie. Il n'y a pas aux yeux de l'auteure de « déterminisme à sens unique, de la technique vers le social ou du social vers la technique », mais « des séries d'interactions et de rétroactions entre l'un et l'autre » qui les redéfinissent réciproquement⁴³⁷. De plus, technique et société étant liées organiquement avec leurs différences chez chacun des auteurs évoqués dans le cadre d'une « méta-construction », l'auteur rejette le principe d'une différence de nature entre société et technique mais renvoie à une différence de degrés de solidité, d'objectivité et de prévisibilité des constituants de celles-ci. A un degré conceptuel si on dépasse la question des postulats des modèles présentés, il y aurait donc une forme de compatibilité des modèles globaux avec des théories plus récentes⁴³⁸.

Du côté des modèles de causalité locale, sont principalement évoqués deux ensembles d'auteurs. Le premier groupe d'auteurs de la causalité locale est tiré de la sociologie des techniques et s'inspirerait des travaux de William Fielding Ogburn tirés de la sociologie des techniques. Le principe retenu ici est celui de la double détermination réciproque du social et la technique⁴³⁹. Elle inclut plus particulièrement les travaux de Seabury Colum Gilfillan sur la notion invention⁴⁴⁰. Le second groupe d'auteurs, inclus à ce stade de la typologie, concerne les auteurs qui travaillent sur en règle générale sur l'innovation en tant que processus social.

⁴³⁴ LEROI-GOURHAN André, *Le geste et la parole*, Volume 1, Paris, A. Michel, novembre 1964, 326 p. et Volume 2, Paris, A. Michel, 1965, 288 p.

⁴³⁵ MUMFORD Lewis (1967-1970), *le Mythe de la machine, Tome 1 : La Technologie et le développement humain et Tome 2 : Le Pentagone de la puissance*. Paris, Fayard, 1974.

⁴³⁶ L'auteure s'appuie sur la réception de Marx chez les sociologues Donald A. MacKenzie et Ron. Westrum. Voir MACKENZIE Donald « Marx and the Machine », *Technology and Culture*, Vol. 25, No. 3. juillet, 1984, pp. 73-502. WESTRUM Ron. *Technologies & Society: The Shaping of People and Things*. Belmont, Wadsworth Pub. Co, 1991, 394 p. Pour aller plus loin, voir par exemple BIMBER, Bruce. « Karl Marx and the Three Faces of Technological Determinism », *Social Studies of Science*, vol. 20, no. 2, 1990, pp. 333–351. ; AXELOS Kostas (1961), *Marx penseur de la technique*, Encre Marine, La Versanne, 2015, 464 p. ; et pour une critique de cette association voir RODRIGO, Pierre. « Marx et la technique », *Philosophie*, vol. 133, no. 2, 2017, pp. 37-51.

⁴³⁷ AKRICH,, 1994, op-cit. pp 116-117.

⁴³⁸ L'auteure prend l'exemple de la double causalité dans les travaux sur la technique de COCKBURN Cynthia, « The Material of Male Power » *Feminist Review*, n° 9, 1981, pp. 41-58.

⁴³⁹ L'auteure reprend à Ron Westrum le qualificatif de « Ogburn Generation» pour décrire ces auteurs. WESTRUM Ron, 1991 op-cit.

⁴⁴⁰ Pour compléter et nuancer cette assertion à l'aune des travaux de Robert K. Merton, voir l'article de DUBOIS Michel, « From Discovery to Invention », *Revue européenne des sciences sociales*, 52-2, 2014, p. 7 – 42.

L'article opère une analyse conjointe de travaux en économie et en sociologie. Du côté de l'économie, sont repris principalement à l'économie de la connaissance en mobilisant le modèle de Nelson, Winter et Dosi⁴⁴¹. Ce modèle économique est comparé à la construction sociale des technologies de Trevor Pinch et Wiebe Bijker⁴⁴². La technique est ici conçue dans son rapport au savoir (dispositifs, savoir, savoir-faire) en ce qu'elle constitue une forme d'état de l'art des problèmes et des méthodes disponibles pour leur résolution... Cette technologie/connaissance peut être « incorporée » dans des artefacts ou dans la pratique quotidienne de tous les acteurs concernés par le développement technologique. Ce savoir peut être propre à un groupe d'acteurs (construction sociale des technologies) une firme ou un secteur industriel (économie de la connaissance) ou avoir une portée plus générale. L'article mentionne paradigmes technologiques de Giovanni Dosi⁴⁴³. Il faudrait sans aucun doute compléter avec la notion de culture, mais le défaut de ces approches est qu'elles traduiraient plutôt les changements technologiques qu'une transformation de la société contrairement aux modèles de causalité globale⁴⁴⁴.

Le troisième grand type de modèle selon cette typologie fait intervenir la notion de réseau et repose sur l'hybridation de la technique et société. Dans ce modèle, où technique et société forment des ensembles indéterminés qui se stabilisent l'un et l'autre, le réseau représente une forme de réponse à l'hétérogénéité de la technique. Pour comprendre ce dernier caractère, la typologie remonte aux travaux de l'historien de Thomas Hugues que nous

⁴⁴¹ Ce modèle économique en question inspiré notamment par Joseph Schumpeter renvoie à l'ensemble des travaux en économie de la connaissance. Sur le modèle proprement dit voir NELSON Richard., WINTER Sydney, *An Evolutionary Theory of Economic Change*. Cambridge, Belknap Press/Harvard University Press, 1982. 400 p. ; DOSI Giovanni « Technical paradigms and technical trajectories: the determinants and directions of technical change and the transformation of the economy », *Research Policy*, 11, 1982 pp. 147-162. DOSI Giovanni, « Sources, procedures and microeconomic effects of innovation », *Journal of Economic Literature*, 26, 1988, pp. 126-173. Plus récemment voir l'ouvrage des trois auteurs DOSI Giovanni., NELSON R., WINTER Sydney, *The nature and Dynamics Capabilities of the Firm*, Oxford, Oxford University Press, 2001, 408 p. Pour un résumé de ce modèle et de son apport, voir par exemple BASLE Maurice, *Approches évolutionnistes de la firme et de l'industrie: théories et analyses empiriques*, L'Harmattan, 1999, 367 p.

⁴⁴² L'article fait référence à la version republiée en 1989 de l'article : PINCH, Trevor J. et BIJKER Wiebe E. , « The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. », *Social Studies of Science*, vol. 14, n°. 3, 1984, pp. 399–441.

⁴⁴³ DOSI, 1982, op-cit

⁴⁴⁴ COUPAYE Ludovic et DOUNY Laurence, « Dans la Trajectoire des Choses », *Techniques & Culture*, 52-53, 2009, pp. 12 – 39.

pouvons facilement associer au modèle de la construction sociale des technologies⁴⁴⁵, ainsi qu'aux travaux de Paul David et de Nathan Rosemberg⁴⁴⁶. Cet apport est nécessaire à l'introduction de la notion d'hétérogénéité des techniques qui amène à circonscrire une forme de coproduction de l'émergence des techniques avec leur implémentation dans le corps social. L'articulation entre les conditions d'émergence des techniques et de leurs réceptions est ce qui caractérise le troisième type de modèles organisés autour du principe qui veut que « la négociation des contenus techniques qui conduit à leur redéfinition, s'accroît la capacité du dispositif à traduire les besoins, aspirations, objectifs supposés de tous ceux qu'il se doit d'intéresser. »⁴⁴⁷ Ce modèle associe les approches précédentes dans un processus sociotechnique unique de développement d'un réseau où chacune des approches joue le rôle d'une « stratégie ». Par la décision sur un contenu technique, l'entité humaine ou non humaine contribue à sa propre définition. La technique apparaît alors comme un espace de redistribution des compétences et où la science intervient pour qualifier les représentants des divers acteurs de ce processus (notamment pour les entités non-humaines). Le réseau permet ici une « entre-définition » des faits techniques sur la base d'un consensus. Cette dernière approche d'une technique où seule la construction d'un réseau permet la prévisibilité et l'irréversibilité du changement technologique se rapproche de la sociologie des techniques en particulier le courant de la sociologie de la traduction à laquelle Madeleine Akirch participe avec Bruno Latour et Michel Callon⁴⁴⁸.

Si l'on devait résumer cette typologie, il y aurait finalement trois manières de comprendre les articulations entre la technique et la société : soit la technique est autonome (système), soit elle est séparée de son environnement mais peut influencer ou être influencée par ce dernier (causalité), soit la technique est une forme de socio-matérialité qui s'articule

⁴⁴⁵ Cf. l'ouvrage collectif codirigé avec Trevor Pinch et Wiebe Bijker, contenant les actes d'un colloque de juillet 1984 à l'université de Twente (Enschede, Pays-Bas), BIJKER Wiebe E, HUGHES Thomas P. et PINCH Trevor J. (eds.), *The social construction of Technological Systems*, Londres, MIT Press, 1987, 470 p. Tout particulièrement le chapitre HUGHES Thomas P. « The Evolution of Large Technological Systems », In. Ibid, pp. 51 – 82.

⁴⁴⁶ Sur la notion d'interdépendance des techniques, nous renverrons pour notre part ici à l'ouvrage ROSENBERG Nathan, 1994 précité. ainsi que DAVID Paul, « La moissonneuse et le robot. La diffusion des innovations fondées sur la micro-électronique » In. SALOMON Jean-Jacques. et SCHMEDER Geneviève (eds) *Les enjeux du changement technologique*, Paris, CPE-Economica, 1986, pp

⁴⁴⁷ AKRICH, 1994, op-cit. p. 126.

⁴⁴⁸ AKRICH Madeleine, CALLON Michel et LATOUR Bruno (éd.), *Sociologie de la traduction : textes fondateurs*, Paris, Mines ParisTech, les Presses, « Sciences sociales », 2006, 401 p.

avec son environnement dans un processus de co-construction (réseau). Appliqué au cyberespace, cette gradation nous permet schématiquement d'aborder les différentes conceptualisations en fonction d'une répartition entre des approches techno-centrées et des approches plus ouvertes à la société⁴⁴⁹. Une manière d'expliquer anachroniquement cette ambivalence de la technique qu'elle constitue est de traiter de la technologie comme une notion socialement construite. La plupart des questions qui portent sur les caractéristiques de la technique génèrent des réponses qui relèvent de type idéologique. Toutefois, cette grille ne permet pas de prendre en compte les aspects discursifs liés au phénomène linguistique analysé, et elle n'établit pas de rapport particulier à la notion d'information, ni la dimension internationale de celui-ci⁴⁵⁰.

2 – La technique comme phénomène social et « international » : nation et civilisation chez Marcel Maus.

Marcel Maus et son oncle Emile Durkheim ont rédigé ensemble une note sur la notion de civilisation en 1913⁴⁵¹, où ils argumentent l'existence de phénomènes « supra-nationaux » en opposition au cadre d'une organisation politique définie (nation, ville...). Ils évoquent ainsi des systèmes complexes et solidaires plus « grands » qui ne sont « ni la chose d'un État, ni d'un peuple ». Au titre de ces phénomènes, les auteurs mentionnent la technologie, mais aussi les discours sur l'esthétique ou encore la linguistique. Plus étendues dans le temps et/ou dans l'espace, ces « aires de civilisation » constituent un « milieu moral » dont la culture nationale ne serait qu'une forme particulière. Marcel Mauss poursuit l'analyse au cours des années 20, dans ses travaux sur la nation⁴⁵².

Il y consacre une partie à l'étude de la technique en tant qu'objet de recherche, évacuant dans un premier temps le caractère commercial de la vie technique au profit des mouvements d'emprunt et de propagation des techniques affirmant que sauf préjugés, manque de moyens ou de volonté, « une société fait tous ses efforts pour adopter et faire siennes les

⁴⁴⁹ Qui ne se résumera pas à la distinction entre technophile et technophobe.

⁴⁵⁰ Quand bien même on y retrouve des prémisses qui serviront également à la communauté épistémique.

⁴⁵¹ DURKHEIM Emile et MAUSS Marcel, « Note sur la notion de civilisation », *L'année sociologique*, n°12, 1913, pp. 46-50.

⁴⁵² Ces travaux ne feront l'objet d'une publication que de manière incomplète et à titre posthume en 1953, MAUSS Marcel, « la nation », *L'année sociologique*, 3ème série, 1953, pp. 7-68.

techniques dont elle constate la supériorité »⁴⁵³. Mauss a poussé l'analyse plus loin en circonscrivant le « phénomène de civilisation » au phénomène social commun à plusieurs sociétés : un rapprochement par essence international ou extraterritorial qui s'opère entre deux sociétés suivant contact prolongé, intermédiaire permanent ou filiation à partir d'une souche commune⁴⁵⁴. Enfin, dans son article consacré aux techniques du corps publié dans le *Journal de psychologie normale et pathologique* en 1935⁴⁵⁵, Marcel Mauss parvient à conceptualiser les techniques en tant qu'acte « traditionnel et efficace ». Il n'y a pas de technique et de transmission sans une tradition, propre à distinguer l'humain des animaux. Cette dernière définition appelle deux remarques : Premièrement, la transmission des techniques apparaît ici comme le véritable marqueur de séparation entre homme et animal. Le sens de la vie technique a donc moins d'importance pour comprendre le social que les mécanismes qui permettent sa transmission. Deuxièmement, cette seule définition demeure parcellaire car elle inclut, notamment pour les techniques du corps, une forme de téléologie ; laquelle réside dans l'adaptation constante à un but (pour le corps : physique, mécanique, chimique). La technique, acte traditionnel efficace, apparaît non comme le seul fait de l'individu mais un produit coconstruit par l'individu, son éducation, la société dans laquelle il se trouve (ainsi que la place qu'il y occupe).

Aux lendemains de la Première guerre mondiale, Marcel Mauss a souhaité travailler sur la figure de « nation » et les rapports entre les nations. Ces travaux sont intéressants car ils présentent la spécificité de s'inscrire dans une forme de filiation avec les travaux d'Emile Durkheim, en étant contemporain de la « naissance » des Relations Internationales en tant que discipline académique. Ces travaux ont notamment abouti à deux textes : d'une part, un article qui sera publiée à titre posthume dans la revue *l'année sociologique* « La nation »⁴⁵⁶ et d'autre

⁴⁵³ Ibid.

⁴⁵⁴ MAUSS Marcel, « Les civilisations. Eléments et formes » in. FONDATION POUR LA SCIENCE - CENTRE INTERNATIONAL DE SYNTHESE (dir.), *Civilisation. Le mot et l'idée*, Paris, La Renaissance du Livre, 1930, pp. 81-108.

⁴⁵⁵ MAUSS Marcel, « les techniques du corps », *Journal de psychologie normale et pathologique*, n°32, 1935, pp. 271-293.

⁴⁵⁶ Op-cit.

part, une communication réalisée en 1920 à Londres « La nation et l'internationalisme »⁴⁵⁷. Ainsi que le montre l'analyse de Frédéric Ramel⁴⁵⁸, ces deux textes sont difficilement détachables de la personnalité et de l'ensemble des œuvres de leur auteur notamment parce qu'ils sont conçus dans une perspective idéologique particulière (ici le pacifisme) mais aussi parce qu'ils sont le reflet d'un état de l'art particulier de la sociologie comme du champs des Relations Internationales inféodé alors au Droit et à la Philosophie⁴⁵⁹. Ces éléments imposeraient à l'auteur une double contrainte qui entraînerait des difficultés méthodologiques voire épistémologique chez Mauss. Frédéric Ramel dépeint un auteur qui, au-delà de ses idées l'ayant conduit à défendre le wilsonisme, constitue un auteur « de transition » dans la sociologie positive des Relations Internationales⁴⁶⁰. Et s'il y a bien, une idée à retenir c'est celle-ci ; non pas au regard de l'histoire, mais au regard des apports et des limites de l'œuvre. En effet, l'idée de transition se retrouve en filigrane dans l'ensemble de l'œuvre : elle passe d'abord par l'usage de l'idée de « nation » que Mauss présente tout d'abord comme une forme de langage nouveau pour désigner un État. Néanmoins, lui-même va mobiliser le concept de nation comme trait d'union entre l'État et la civilisation : « Nous entendons par nation une société matériellement et moralement intégrée, à pouvoir central stable, permanent, à frontières déterminées, à relative unité morale, mentale et culturelle des habitants qui adhèrent consciemment à l'État et à ses lois »⁴⁶¹.

Autrement dit, la conception de Marcel Mauss de la nation se traduit dans une représentation par l'individu d'une société matériellement et moralement « intégrée ». La nation « maussienne » décrit ainsi un stade de développement particulier d'une société fondée

⁴⁵⁷ Communication publiée une première fois dans les actes de la manifestation : MAUSS Marcel, « The Problem of Nationality », *Proceedings of the Aristotelian Society*, Londres, 1920, pp. 242 - 251. Puis reproduite dans les œuvres complètes de Marcel Mauss : MAUSS Marcel, *Oeuvres, Tome III. Cohésion sociale et division de la sociologie*, Paris, Les Éditions de Minuit, coll. Le sens commun, 1969, pp. 626-634.

⁴⁵⁸ RAMEL Frédéric, « Marcel Mauss et l'étude des relations internationales : un héritage oublié », *Sociologie et sociétés*, vol. 36, n° 2, 2004, pp. 227-245.

⁴⁵⁹ A ce sujet, Frédéric Ramel prendra soin de bien distinguer l'œuvre de Mauss des approches postérieures : d'une part, Mauss considère l'interdépendance internationale comme un phénomène permanent ; là où Joseph S. Nye et de Robert Keohane en font un marqueur de modernité post-1945. D'autre part, Mauss n'établit pas de primauté entre les différents facteurs pour analyser les interdépendances ; là où la technique et l'économie priment pour les penseurs de l'interdépendance dans les années 70 (Frédéric Ramel prend l'exemple de David Mitrany).

⁴⁶⁰ Frédéric Ramel retient ici l'idée positive comme une forme « classique » d'épistémologie conduisant à élaborer une science de la société « sur le modèle des sciences de la nature, comme la physiologie ou l'organicisme, et sur la base de faits empiriques nombreux et précis », Ibid.

⁴⁶¹ MAUSS, « La nation et l'internationalisme », op-cit.

sur une unité culturelle relative où la culture nationale ne joue finalement qu'un rôle mais n'en constitue pas pour autant l'ensemble fondé autant sur l'intégration interne que sur l'unité économique et la « croyance ». La nation apparaît alors comme une recherche d'un ordre né de l'opposition (mais également source d'opposition). Pour Mauss, cette opposition semble être l'essence de la nation qui se définit d'abord elle-même par « la réaction face à l'étranger » (à la fois à l'extérieur par la définition de ses frontières mais aussi à l'intérieur en gommant les divisions antérieures). L'unité économique est perçue ici comme une résultante pathologique du réflexe de protection induit par le mécanisme « intégration/exclusion » qui accapare excessivement la vie économique. Pour Mauss, la croyance est un agrégat illusoire de trois représentations : la « race », la « langue » et la « civilisation », soit la valorisation de l'appartenance (et ce quel que soit le critère relatif) par rapport à l'appartenance à une autre nation⁴⁶². La nation fondée par la transmission du préjugé est regardée comme un produit : « Alors que c'est la nation qui fait la tradition, on cherche à reconstituer celle-ci autour de la tradition ». La nation est donc ainsi le résultat subjectif de mouvements internes et externes qui viennent justifier aux yeux de Mauss l'intégration de la vie « entre les nations ».

En bon héritier du positivisme en sociologie, Mauss mobilise le concept de milieu pour décrire ce domaine dans un raisonnement *a fortiori* : « Une société qui est déjà un milieu pour les individus qui la composent, vit parmi d'autres sociétés qui sont également des milieux. Donc, nous nous exprimerions correctement si nous disions que l'ensemble des conditions internationales, ou mieux intersociales, de la vie de relation entre sociétés, est un milieu des milieux »⁴⁶³. Ce « milieu des milieux » permet pour Mauss de conduire une étude des « structures en mouvement », et notamment « l'évolution des fonctions relatives aux structures nationales » pour circonscrire des phénomènes d'interdépendance entre les différentes nations (que Mauss fixe, sans pouvoir réellement les évaluer, à l'économie libérale et aux aspirations pacifistes des peuples). La nation est structure en mouvement vouée à absorber au gré de son évolution différents autres groupes sociaux suivant l'élargissement des repères identitaires et donc l'intensification des civilisations par l'accroissement des phénomènes de civilisation : c'est là que nous retrouvons l'exemple des techniques et de la tradition des techniques (progression des réseaux de communication, nouveaux moyens de diffusion de la culture...) que nous évoquions précédemment. Mauss nuance son approche en

⁴⁶² Mauss ne semble pas ici prendre la mesure des débats.

⁴⁶³ MAUSS, « La nation », op-cit, p. 43.

évoquant le fait que ce phénomène peut créer des tensions qu'il analyse comme autant de refus de l'interdépendance internationale. Dans sa lecture de Mauss, Frédéric Ramel opère justement une comparaison sur ce point avec les travaux de Norbert Elias⁴⁶⁴ tant sur le phénomène de civilisation qui induit un changement formel d'organisations sociales vers davantage de globalité tant dans l'analyse des phénomènes qu'ils rassemblent tout deux sous le concept de régression « vers des appartenances identitaires d'ordre nationaliste » pour Mauss, ou de régression des « habitus nationaux face à l'intégration des États » pour Elias.

Néanmoins, les différents exemples retenus par Marcel Mauss inciteraient à établir une comparaison avec un auteur plus ancien⁴⁶⁵, Gabriel Tarde et sa sociologie de l'imitation. En effet, si l'approche de Mauss retient à titre d'exemple plusieurs domaines normatifs comme la technique, la linguistique, l'esthétique ou le Droit. Sur ce dernier, le point de départ de la démonstration est quasiment le même chez les deux auteurs : si Tarde affirme que « Le Droit est de tous les domaines de la vie sociale celui où la spéculation philosophique s'est le moins exercée de nos jours. »⁴⁶⁶, de son côté Mauss affirme que « les phénomènes juridiques sont [...] parmi ceux qui, avec la langue, s'empruntent le moins et sont le plus caractéristiques de sociétés données »⁴⁶⁷. Marcel Mauss nous décrit les « phénomènes de civilisation » liés au Droit comme les traités internationaux formés par des sociétés ayant atteint un certain stade de développement et possédant également un impact à un niveau interne⁴⁶⁸.

Prenant le modèle des langues, le paradigme de l'imitation de Tarde permet d'accéder à un degré de granularité plus profond dans l'analyse : celui des effets de structure et de la diffusion des normes dans plusieurs environnements juridiques différents. Premièrement, c'est avant tout la démystification de la nature irrésistible de l'idée du Droit pour toute société

⁴⁶⁴ Frédéric Ramel fonde son analyse sur essentiellement deux ouvrages de Norbert Elias. ELIAS Norbert, *La Société des individus*, Paris, Fayard, 1991 et ELIAS Norbert *La Dynamique de l'Occident*, Calmann-Lévy, 1975.

⁴⁶⁵ Le parallèle est d'autant plus intéressant qu'il est établi avec un adversaire d'Emile Durkheim à qui ont été adressé des reproches similaires à ceux adressés à Marcel Maus : l'ambition trop grande de leurs théories voire une forme d'universalisme, et une tendance à la confusion des champs anthropologiques et sociologiques pour Mauss ; psychologiques et sociologiques pour Tarde.

⁴⁶⁶ TARDE Gabriel, *Les transformations du droit. Étude sociologique* (1891), Paris, Berg International Éditeurs, 2e édition, 1994, 216 pp.

⁴⁶⁷ MAUSS, « la nation » op-cit, Vème partie, pp. 618-620

⁴⁶⁸ Mauss adopte l'exemple de la propriété intellectuelle : « Ainsi il fallut que la Russie modifiât son droit de propriété littéraire pour pouvoir accéder à la Convention de Berne »

humaine : « De telle sorte que, si, par impossible, l'idée du Droit venait à disparaître aujourd'hui de l'humanité, elle renaîtrait fatalement demain »⁴⁶⁹. Inspiré par Leibniz, Tarde envisage l'histoire comme une succession de modèles aptes à susciter une imitation par un grand nombre d'individus, où chacun vient copier les imitations (qu'il admire) choisies à plusieurs sources tout en les aménageant à sa manière. Les imitations ne sont pas nécessairement parfaites. Ainsi, par exemple la justice pénale procède de variations d'imitation autour de l'idée de justice domestique assimilée à la réaction défensive face à l'acte criminel, avant la seule idée de vengeance (laquelle n'est qu'une source secondaire même si l'auteur la reconnaît plus « visible »). Ainsi, pour Gabriel Tarde, le lien social est davantage cyclique : il se caractérise à la fois par l'imitation, la résistance qu'elle engendre et l'adaptation dans le compromis jusqu'à ce qu'un nouveau modèle arrive. Dans cette approche, la civilisation n'apparaît pas comme une figure forcément pacifique ou perçue positivement ou continue : elle implique simplement une transformation par diffusion d'un modèle de référence. Le conflit n'est pas une forme d'exception à une loi de diffusion de la norme mais bel et bien une partie de la loi elle-même. Le concept d'imitation de Tarde⁴⁷⁰ peut donc apparaître comme une approche complémentaire de nature à opérer des analyses plus profondes des interdépendances entre les sociétés identifiées par Maus. Et ce, en discriminant ce qui relève de « l'interdépendance » d'une simple « similitude » tout en lui permettant de prendre en compte l'intérieur des sociétés et notamment l'importance des conditions sociales dans la diffusion normative des techniques.

⁴⁶⁹ TARDE, op-cit, p. 23.

⁴⁷⁰ Gabriel Tarde dans *Les transformations du droit*, précise dans la seconde partie de ses conclusions que les similitudes dans « Il n'est pas une similitude dans l'Univers qui n'ait pour cause l'une de ces trois grandes formes, superposées et enchevêtrées, de l'universelle répétition : l'ondulation pour les phénomènes physiques, l'hérédité pour les phénomènes vivants, l'imitation pour les phénomènes sociaux proprement dits. », op-cit, p.169-170. Ceci pourrait laisser à penser que l'autonomie de l'individu n'a pas beaucoup de place, néanmoins il nuance son approche sur les similitudes en mettant en avant leur caractère accidentel : « Mais toutes les similitudes, même d'origine sociale, que présentent les législations ou, pour mieux dire, les activités juridiques des divers peuples, n'ont pas l'imitation pour cause. Beaucoup relèvent de la logique. Si l'homme est imitatif, c'est parce qu'il est inventif ; [...] Et si l'homme est inventif, c'est qu'il est logique. Logique ou inventif, c'est tout un, au fond. Une invention, une découverte n'est que la réponse à un problème, et cette réponse consiste toujours à rattacher les uns aux autres, par le rapport fécond de moyen à fin, des modes d'action précédemment séparés et stériles, ou à rattacher les uns aux autres, par le rapport non moins fécond de principe à conséquence, des idées ou des perceptions qui, auparavant, semblaient n'avoir rien de commun », op-cit p. 185. L'ensemble de ces propos fait référence à son ouvrage *les lois de l'imitation* paru en 1890. TARDE Gabriel, *les lois de l'imitation*, Paris, F. Alcan, 1890, 431 p.

B – Information et technologie : un héritage matérialiste à dépasser.

Pour parler d'information, il serait donc bien plus simple d'employer un vocabulaire tiré de l'univers matériel ou technique surtout quand il s'agit de sécurité. Ainsi, si l'héritage matérialiste de la technique ou de l'information ne suffisent pas à les décrire entièrement, il conditionne visiblement la domination de représentations basées sur la matérialité pour tous les objets qui en sont issus ou qui peuvent être perçus comme tels⁴⁷¹. On pourra ainsi trouver sans peine des utilisations abusives de certaines qualifications consacrées de manière légale ou prétorienne : le terme de « vol » de données pour une simple copie illégale, le « cybercrime » pour des choses qui ne relève que du délit. Comme si l'absence de caractère « palpable » de ces comportements les rendait « pires » en dépit d'une matérialité bien réelle. Le sentiment d'absence du réel discriminera les objets dits « virtuels » et favorisera des approches et les acteurs « techniciens » de l'information. Car la technique constitue la seule de nature à favoriser la maîtrise de l'humain sur cet environnement « hostile » et « complexe ». Notre propos ne peut pas faire ici l'économie de la difficulté d'avoir une image particulière de l'origine de la technique en tant qu'objet aux contours définis qui conditionne la lecture des définitions du cyberspace. Et c'est encore plus vrai quand il s'agit du poids des représentations de la technique lorsqu'il s'agit d'information.

1 – De la « structure » à la « fonction » : les origines matérialistes de l'information.

Ce n'est qu'avec les travaux de Shannon et Weaver, autour d'une « théorie de l'information » s'intéressant à la transmission des messages, qu'une première définition du concept d'information commence à être posée⁴⁷². Dans cette théorie, le sens de l'information doit être écarté. L'information ne vaut que comme un support⁴⁷³. Dans un ouvrage de 2008

⁴⁷¹ GUCHET Xavier, « L'objectivité technologique », *Pour un humanisme technologique*, Paris, PUF, « Pratiques théoriques », 2010, pp. 133-190.

⁴⁷² Plus précisément, vérifier l'intégrité des messages transmis ou la conformité du message reçu, SHANNON, Claude, E. et WEAVER, Warren, *The Mathematical Theory of Communication* (1934), University of Illinois Press, 1963, 125 p.

⁴⁷³ Sur la valeur politique de l'information notamment par le biais du développement de la cybernétique, voir GEOGHEGAN, Bernard D. « The Historiographic Conceptualization of Information : A Critical Survey », *IEEE Annals of the History of Computer*, vol. 30 n°1, 2008, pp. 66-81.

tiré de sa thèse de doctorat⁴⁷⁴, Mathieu Triclot reprend cette genèse de l'idée de message et retrace cette interprétation « physicaliste » de la notion d'information conduisant à la disparition de la structure au profit de la seule fonction de l'information⁴⁷⁵. Dans cette vision, le réel est réductible à une forme de code. Si l'information est entendue ici sous un prisme spécialisé, le concept sera repris dans les mouvements cybernétiques des années 40-50 que nous avons évoqués⁴⁷⁶ (non plus véritablement comme un code mais davantage comme un signal).

« Le principe même de la cybernétique était bien de contrôler le fonctionnement de machines physiques à partir justement de l'information qu'elles tiraient de leur structure interne et de leur interaction avec le milieu dans lequel elles étaient plongées. »⁴⁷⁷

Dans une vision matérialiste, la nature de l'information évolue à travers son support. Traiter uniquement de la partie « fonctionnelle » au sens de la cybernétique ne suffirait ainsi qu'à rendre compte d'une partie de l'information. Cette idée se retrouve notamment dans l'hypothèse de « boîte noire »)⁴⁷⁸. Le message est pris en compte comme une suite de caractères où chaque signe se formule sous la forme d'une probabilité.

Gérard Chazal ne retient l'information que comme un « état identifiable en tant que tel d'un dispositif physique » en retenant exclusivement le déterminisme du support pour fournir finalement une information neutre appréhendable par son environnement en tant que telle et confirme un caractère ultime à la perception du sujet : l'information n'existe que dans la confrontation physique avec le sujet et il n'existe pas d'information non-perceptible. Ce n'est pas tant que le sujet puisse tout percevoir, mais simplement que le caractère d'« information » ne peut être attribué qu'aux choses perçues. Il y a dans cette « philosophie de la donnée brute » un obstacle ontologique qui la rend inopérante pour notre objet. Sur la forme, la démonstration accomplit le pendant de ce qu'elle dénonce : Si elle semble reprocher à la cybernétique de ne

⁴⁷⁴ Essentiellement mobilisé ici dans sa seconde et sa troisième partie, voir TRICLOT Mathieu, *Le Moment cybernétique, la constitution de la notion d'information*, Champ Vallon, 2008, 422 p.

⁴⁷⁵ Dans le même sens : SEGAL Jérôme, op-cit.

⁴⁷⁶ Voir en particuliers les auteurs dit de la « seconde cybernétique » John von Neumann et William Ross Ashby. NEUMANN (VON) John, *L'Ordinateur et le cerveau* (1958), Flammarion, 1999, 125 p. / ASHBY William Ross, *An Introduction to Cybernetics* (1957), Martino Fine Books, 25 janv. 2015, 306 p.

⁴⁷⁷ CHAZAL Gérard, op-cit.

⁴⁷⁸ Cf. supra.

traiter qu'un aspect de l'information au travers d'une conception fonctionnelle de l'information, le déterminisme matériel qu'elle tente de lui imposer n'en est pas moins négliger la nature de l'information.

Sur le fond, il y a un paradoxe à vouloir présenter l'information comme le fruit de la perception du sujet en prétendant cette information-perception est par nature extrinsèque. De fait, cette conception ne peut répondre à l'ensemble des questions techniques, sémantiques ou sociales soulevées dans le cadre de « philosophie de l'information »⁴⁷⁹. L'importance de cet héritage matérialiste de l'information sera tel qu'il impactera le discours sur celle-ci dans tous les registres et les variations de celui-ci, y compris dans ses versions les plus critiques... De plus, cet héritage matérialiste contribuera notamment à une forme d'hyperspecialisation des champs disciplinaires quand il s'agira d'aborder la technique et l'information.

2 – Information et progrès technique : le rôle clef des technologies de l'information.

« [...] Le croyant progressiste fonde sa confiance dans un avenir meilleur sur le postulat suivant : le progrès de l'esprit humain, attesté par les progrès observables des sciences, dont le caractère cumulatif est reconnu, constitue à la fois la preuve irrécusable de l'existence du progrès, la condition déterminante de tous les progrès et le modèle du Progrès pris dans son sens absolu, centré sur la certitude que la condition humaine, voire la nature humaine, est en voie d'amélioration, de transformation graduelle vers le mieux. »⁴⁸⁰

En parallèle de cet héritage, l'information s'est retrouvée associée à l'idée de progrès⁴⁸¹. C'est notamment le cas dans les travaux de Pierre-Alexandre Taguieff⁴⁸². Ce dernier décrit le progrès comme l'un des deux piliers de la Modernité avec le culte de l'avenir. Le progrès n'a pas réellement de définition explicite : quand les auteurs s'essayent à le

⁴⁷⁹ Pour une synthèse de ces questions, voir notamment la conférence : FLORIDI Luciano, « Where are we in the philosophy of information ? », University of Bergen, Norway. 21 juin 2016.

⁴⁸⁰ TAGUIEFF Pierre-Alexandre, « L'idée de progrès une approche historique et philosophique » suivi de « Eléments de Bibliographie », *Les Cahiers du CEVIPOF*, septembre 2002 / 32, 137 p

⁴⁸¹ Sur cette association voir par exemple : NISBET Robert A., *History of the Idea of Progress*, Transaction Publishers, 1980, 370 p. voir également : GODIN Benoît, *Innovation Contested – The Idea of Innovation Over the Centuries*. Londres, Routledge, 2015, 354.

⁴⁸² Si on pense notamment TAGUIEFF Pierre-Alexandre, « L'idée de progrès une approche historique et philosophique » suivi de « Eléments de Bibliographie », ibid. Publication qui sera reprise dans l'ouvrage éponyme TAGUIEFF Pierre-Alexandre, *L'idée de progrès une approche historique et philosophique* (2004), coll. Champs/essais, Flammarion, 2011, 445 p.

caractériser ne peuvent faire l'économie d'une sémantique extrêmement large. Néanmoins, Taguieff relève que le progrès entendu au sens le plus commun n'est célébré qu'à la condition qu'on puisse lui reconnaître une certaine utilité, et une utilité immédiate qu'illustre les places données aux technologies de l'information comme marqueurs de ce même progrès, auquel correspond également un culte de la vitesse et du temps court. Ainsi, toute la problématique réside dans le fait de démontrer que cette acceptation nouvelle du progrès forme le cadre utopique moderne dans lequel l'information peut être valorisée⁴⁸³.

Plus spécifiquement, le progrès technologique marqué par le succès de l'information est-il toujours dans l'histoire du Progrès ? En répondant, sur un culte de la vitesse⁴⁸⁴, l'idée de progrès serait ainsi devenue libérale en lieu et place d'une posture critique et révolutionnaire⁴⁸⁵. Le progrès est ainsi passé d'une vision globale à une approche qualifiée de « méliorisme », où seuls certains progrès sont valorisables : des progrès partiels, contingents, spécifiques ou/et partiels dépendants de la volonté humaine. C'est en cela que l'impératif d'un progrès global automatique fondé sur la nécessité passe par la faculté de choix et donc par la liberté⁴⁸⁶. C'est donc dans ce contexte, que Taguieff cherche à repenser politique un progrès en résistance au culte de la vitesse indépendant de la vision d'une rupture totale avec le passé et de l'inscription du progrès dans quelque loi naturelle. Néanmoins, on ne saurait faire l'économie d'une idée-force fondamentale pour comprendre le Progrès au sens de Taguieff et venir éclairer ici la notion d'information sous un aspect que l'auteur ne met pas directement en valeur : le savoir est pouvoir. Autrement dit, l'idéologie selon laquelle la science (donc la technique) résoudra(ont) tous les problèmes de l'humain.

Le rapport entre science et puissance est obtenu chez Taguieff par un basculement du temps vers le futur et donc un rejet de l'idée d'un temps providentiel. Le progrès du savoir et

⁴⁸³ Sur l'idée de vitesse et de développement technologique, nous renverrons également aux travaux de Paul Virilio. En particulier, VIRILIO Paul, *Vitesse et Politique*, Paris, Galilée, 1977, 151 p.

⁴⁸⁴ L'auteur nomme cette tendance le « mouvementisme » ou le « bougisme », soit le culte du mouvement pour le mouvement (op-cit p. 14).

⁴⁸⁵ Pierre-Alexandre Targuieff fait notamment référence à l'ouvrage suivant : AYRES Robert U. , *Information, Entropy and Progress : A New Evolutionary Paradigm*, New York, American Institute of Physics, The AIP Press, 1994, 301 p.

⁴⁸⁶ L'auteur prend ici soin de se prémunir contre le nihilisme porté par la volonté comprise au sens « heideggerien » du terme, ainsi que de la vision « prométhéenne » de cette même volonté. Page 76, il décrit cette volonté comme le fait de vouloir sans « *ubris* » (l'auteur faisant ici référence à l'hubris/hybris grec : orgueil, démesure, excès).

l'accroissement du pouvoir sont les deux branches du moment baconien qui repose sur cette contraction du temps, lequel conduit l'être humain en marche comme un seul individu vers la synthèse de tous les progrès partiels présentés comme une forme de perfection (vérité, liberté, justice, bonheur)⁴⁸⁷. Dans cette acceptation, et même si l'auteur ne le formule pas ainsi car ce n'est pas son objet, l'information, médium du savoir, est au fondement de toute forme d'évolution du monde social fondée sur l'idée du progrès, il en résulte qu'elle est à la fois sa base, sa « condition déterminante » et donc un « modèle » pour comprendre le monde social.

En effet, indépendamment de servir l'idée de progrès, les représentations de l'information sont utilisées pour servir différentes compréhensions du monde social. Cette vocation idéologique du substantif « information » transforme ce dernier en allégorie d'autres idées où le rapport à l'information est souvent conjoncturel ou instrumental. La prise en considération du développement des technologies de l'information et de leur diffusion comme une valeur globale pour ce qui relève de l'aspiration à vivre ensemble. Dans ces utilisations, l'information apparaît ainsi comme a minima comme une coïncidence ou comme l'outil et le vecteur d'un processus plus anciens réactualisés. Le phénomène peut également prendre le nom de l'information, mais plus souvent on insistera sur l'information comme un outil. Ces différents travaux ont en commun de penser un nouvel ordre social est produit à travers les usages des technologies⁴⁸⁸.

Le premier d'entre eux est la société de l'information. Le consensus actuel autour de la société de l'information décrit ce nouvel ordre social comme celui de la société post-industrielle⁴⁸⁹. Cette société post-industrielle aurait pour caractéristiques la transition d'une

⁴⁸⁷ Taguieff , fait ici référence à la liste inachevée des merveilles naturelles évoquée par Francis Bacon à la fin de *la Nouvelle Atlantide* (1627) que nous avons déjà évoqué. Les progrès ultimes du savoir permettront la vie quasiment éternelle, la jeunesse éternelle, augmenter la force et l'activité. (...). Transformer la stature. Transformer les traits. Augmenter et éléver le cérébral. Métamorphose d'un corps dans un autre. Fabriquer des espèces nouvelles. Transplanter une espèce dans une autre. (...). Rendre les esprits joyeux, et les mettre dans une bonne disposition. (...). cf. BACON Francis, *La Nouvelle Atlantide*, op. cit.

⁴⁸⁸ Pour une synthèse de ces différentes approches, notamment le dialogue entre les approches positivistes et critiques, voir la controverse entre réalisme et constructivisme autour de la société de l'information : ISCHY Frédéric, « La « société de l'information » au péril de la réflexion sociologique ? », *Revue européenne des sciences sociales*, XL-123, 2002

⁴⁸⁹ Il faut noter que ce consensus a été pris malgré les origines assez variées de la notion de « société de l'information ». Voir notamment : MATTELART Armand, « L'âge de l'information : genèse d'une appellation non contrôlée ». *Réseaux*, 101, 2000, pp 21-52 ; MATTELART Armand (2001), *Histoire de la société de l'information*, Paris, 4^{ème} édition, La Découverte, juillet 2010, 128 p

économie de biens vers une économie de services, l’importance accordée à la codification des connaissances en matière d’innovation technologique et enfin la mise au point d’outils technologiques pour l’analyse systémique et la prise de décision⁴⁹⁰. Même s’il en existe de nombreuses définitions⁴⁹¹, il faut souligner que l’on retrouve dans le discours essentiellement une acception « mélioriste »⁴⁹². En effet, il s’agit souvent de faire « mieux » à l’aide des technologies de l’information dans une perspective essentiellement à court terme. De l’autre côté de ce même paradigme, se trouve la société de la connaissance⁴⁹³ (que nous rapprocherons ici de la « société des savoirs » sans nous attarder les nuances entre ces deux termes). Reprenant la diffusion des technologies de l’information à la notion précédente, cette société de la connaissance met l’accent sur les processus de savoir, d’innovation et d’expertise qui façonnent une nouvelle forme d’économie du savoir portée par la technique et qui possède de nouvelles pratiques dans son rapport à l’information (informatique décisionnelle, intelligence économique, diffusion des connaissances...). La différence entre le cyberespace et ces éléments tient dans le fait que ce dernier se limite pour le moment à l’approche substantiviste et nominaliste que nous avons évoquée⁴⁹⁴. Pour le reste, des questions similaires ressurgissent⁴⁹⁵ : le cyberespace est-il une rupture ? Une continuité d’une rupture précédemment entamée ? Est-ce seulement une évolution ? Quelles peuvent être ses limites ? A quand remonte-t-il ? Plus encore, le cyberespace reprend également une partie des critiques adressées à la société de l’information dans son impossibilité de la définir et la mesurer.

⁴⁹⁰ BELL, Daniel, « The Social Framework of the Information Society » in DERTOUZOS, M.L., MOSES Joel . (eds), *The Computer Age : a Twenty-Year View*. Cambridge, MIT Press, 1979, pp 163-211.

⁴⁹¹ Même si elle un peu datée, une précieuse lecture ici est l’ouvrage BENIGER James R., *The Control Revolution Technological and Economic Origins of the Information Society*, Harvard University Press, 1986, 436 p. ainsi que l’article BENIGER James R., « Information Society and Global Science », *The ANNALS of the American Academy of Political and Social Science*, 495(1), 1988 pp. 14–28.

⁴⁹² A l’image de l’idée que nous décrivions à partir des travaux de Pierre-Alexandre Taguieff. TAGUIEFF op-cit. Frédéric Ischy parle préféablement du « développementalisme » voir d’une forme de darwinisme. ISCHY, op-cit. ,

⁴⁹³ Le terme *Knowledge Society* est introduit pour la première fois en 1969, il est donc antérieur au terme cyberespace, néanmoins contrairement à ce dernier, il demeure spécifique à certains champs comme l’économie et la gestion. Pour l’œuvre à l’origine du terme, voir, DRUCKER Peter, F. (1969), *The Age of Discontinuity: Guidelines to Our Changing Society*, Transaction Publishers, déc. 2011, 420 p.

⁴⁹⁴ Même si comme le cyberespace, une société de l’information voire l’information seraient parfois perçues comme des « concepts creux », « ambivalents », ouverts à tous les « paradoxes ».

⁴⁹⁵ Ces questions se retrouvent dans la plupart des modèles de compréhension de l’impact des techniques sur la société ou les organisations : société de l’information, de la connaissance, des savoirs, mais aussi révolution numérique, révolution des affaires militaires, pédagogie numérique...

D'autre part, ils semblent s'alimenter à partir des mêmes représentations : le déterminisme technique, le mythe d'un nouvel âge et/ou d'une nouvelle civilisation⁴⁹⁶...

Ces expressions ne sont finalement que le produit d'un contexte : cette période d'environ trente ans entre la fin des années 60 et la fin des années 90, où tout le secteur de l'informatique a entraîné une émergence de nombreux termes dont celle du cyberespace. Sur ces deux expressions, la plupart des auteurs durant les années 2000 portent un regard assez critique. La grande diffusion de ces expressions parmi de nombreux secteurs différents avec une dimension polysémique leur donne une apparence de « neutralité », laquelle est remise en cause à travers les paradigmes de la production et du mythe⁴⁹⁷. Au croisement du cyberespace et de la société de l'information (ou représentée comme telle), se trouve la conception de Manuel Castells souvent reprise ou citée parmi les auteurs qui abordent le cyberespace⁴⁹⁸. L'approche de ce dernier se fonde essentiellement sur un paradigme de la production ainsi que de la culture. A la base de la réflexion de Manuel Castells réside le phénomène de l'invention de nombreuses technologies à partir des années 70 qui ont eu pour conséquences le développement de l'entreprise en réseau, un accroissement (et une accélération) de la mondialisation des capitaux financiers et une nouvelle division du travail fondée sur la différence d'adaptabilité entre « interacteurs » (travailleurs chargés d'animer les réseaux) et « interagis » (travailleurs de l'industrie ou du secteur des services, en marge desdits réseaux). Pour Manuel Castells, ces conséquences forment l'origine des mouvements sociaux et l'émergence d'une culture spécifique dite de la « virtualité réelle ». Cette virtualité réelle constitue pour lui une base nouvelle des activités de la société fondée sur la maîtrise sociale des outils technologiques.

⁴⁹⁶ Partant de ce constat, le « cyberespace » de 1984 pourrait être regardé en partie comme une société de l'information ou de la connaissance selon l'angle de vue porté sur l'œuvre et son esthétique générale...

⁴⁹⁷ Sur cette double remise en cause, voir notamment : BRETON Philippe, PROULX Serge, *L'explosion de la communication : la naissance d'une nouvelle idéologie*, Paris, La Découverte, 1993, 323 p. ; GEORGE Éric et GRANJON Fabien, *Critiques de la société de l'information*, Paris, L'Harmattan, 2008, 268 p. ; NEVEU Éric, *Une société de communication ?*, Montchrestien, 2011, 160 p.

⁴⁹⁸ *La Galaxie Internet* publié en 2002, a déjà fait l'objet d'une référence au moment de parler d'Internet (Cf. Supra). Sur la société de l'information en particulier, l'œuvre la plus citée de Manuel Castells est : CASTELLS Manuel (1996), *L'Ère de l'information. Vol. 1, La Société en réseaux*, Paris, Fayard, 1998, 613 p. Les volumes 2 et 3, *Le pouvoir de l'identité* et *La fin du millénaire*, font généralement l'objet de moins de commentaires quand il s'agit d'aborder la société de l'information en tant que telle ou le cyberespace.

Autrement dit, la culture s'entend ici comme le produit de la communication et la communication comme nouveau mode de production (ce qui vient partiellement gommer la séparation entre la réalité et ses représentations)⁴⁹⁹ ⁵⁰⁰. Dès lors, on peut comprendre le paradoxe de l'engouement suscité par l'approche de Manuels Castells chez les personnes travaillant sur le cyberespace, car au fond celle-ci traduit parfaitement la confusion de signification qui règne entre la nature idéologique du cyberespace et ses représentations spatiales et techniques dominantes. Laquelle confusion vient excuser le déterminisme technique de ces mêmes acteurs au privilège d'une logique de structure en lieu et place d'une action politique. Ce que Manuel Castells traduit dans sa société des réseaux comme la prééminence de la morphologie sociale sur l'action sociale⁵⁰¹.

C – Structure d'une fiction techno-politique : le pouvoir évocateur du cyberespace.

Le cyberespace permet d'interroger les places de l'information et de la technique dans une représentation du monde teintée de matérialisme. Toutefois, il faut pouvoir en restituer un dernier aspect : le fait que le cyberespace existe quasiment uniquement aux plans des idées. Le cyberespace est une fiction. Cet aspect éclaire la transition entre le mot « cyberespace » et le phénomène linguistique de sa prolifération. La sociologie de la technique, même ouverte sur l'international, ne peut pas tout à fait saisir ce dernier. C'est avant tout un problème d'objet. Ici la question n'est plus de comprendre la technique mais plutôt le discours sur une technique particulière. En tant que tel, ce discours opère une forme de médiation entre la société et la technique. Il permet en outre de décrire son pouvoir évocateur malgré l'absence de définition technique réalisable. En effet, le cyberespace comme phénomène du langage représente la technique informatique plutôt qu'il ne la qualifie. Pour pouvoir saisir les liens entre cyberespace et discours, il faut pouvoir considérer que la technique qui est évoquée dans le cyberespace perd son caractère de fait. Elle doit être placée au second degré de l'analyse.

⁴⁹⁹ « La culture étant médiatisée et mise en œuvre à travers la communication, les cultures elles-mêmes, c'est-à-dire nos systèmes historiquement produits de croyances et de codes, sont radicalement transformées et le seront encore davantage par le nouveau système technologique » CASTELLS, op-cit. p. 357.

⁵⁰⁰ Pour une critique plus complète de la manière dont Manuel Castels parvient à cette conclusion : GARNHAM Nicholas, GAMBERINI Marie-Christine (trad.), « La théorie de la société de l'information en tant qu'idéologie : une critique ». In: *Réseaux*, volume 18, n°101, 2000 pp. 53-91

⁵⁰¹ CASTELLS, op-cit., p 525.

C'est notamment le postulat des travaux sur la technique de Lucien Sfez⁵⁰². Lesquels reposent sur la distinction entre les objets techniques et les discours qui en parlent. Les techniques sont toujours accompagnées de discours construit par une collusion du technique et politique (« techno-politique »). La fiction ici n'est plus celle de la littérature mais une fiction politique. Il s'agit là de la co-construction d'un discours et d'un ordre social par un type discours qui en lui-même le produit. Ces fictions de la technique ont un contenu principalement idéologique. Elles ne reposent pas sur une démonstration mais au contraire sur une forme de narration. Une prise de position sur la technique n'est pas justifiable hors du domaine de la croyance et des idées. Ce discours particulier se voit doté d'une structure fictionnelle ainsi que d'un domaine qui ressemble celui de la fiction. Un tel domaine comprend le vraisemblable, le possible, le conjoncturel, l'empirique et la croyance collective. Toutefois, malgré l'étendue du domaine de ce type de discours, ceux-ci sont improches à la constitution d'un imaginaire et ne proposent qu'une collection d'images symboliques (une « imagerie » de symboles plutôt qu'un « imaginaire » symbolique). Dès lors, l'image de la technique n'aurait pas de pouvoir symbolique suffisant pour être instituante de la société dans son ensemble et sa capacité d'influence se limiterait à quelques experts et aux grands corps de l'État.

C'est peut-être sur ce point qu'il faut réagir. Si on peut admettre que la technique doit se comprendre comme discours et admettre son « mariage morganatique » avec le politique, il faut enrichir cette lecture à partir d'autres travaux en histoire des idées sur la technique qui évoquent la réception idéologique de la technique. Il faut ici penser au rôle de la technique par rapport à la puissance présent dans la littérature au début du 20^{ème} siècle et qui préfigurent l'État total⁵⁰³. En particulier, la croissance d'un État négateur des droits de l'individu par l'institution de la technique appliquée notamment à la chose militaire. Cette perspective « totale » de la technique est particulièrement présente dans les études portant sur la domination. Il est possible de se référer par exemple à Herbet Marcuse.

« L'a priori technologique est un a priori politique dans la mesure où la transformation de la nature entraîne celle de l'homme, et dans la mesure où les "créations faites par l'homme" proviennent d'un ensemble social, et où elles y retournent. On peut toujours dire que le machinisme de l'univers technologique est "en tant que tel" indifférent aux fins politiques - il peut révolutionner ou il peut

⁵⁰² En particulier SFEZ Lucien, *Technique et idéologie. Un enjeu de pouvoir*, Paris, Le Seuil, 2002, 336 p. voir également du même auteur et la même année, « La technique comme fiction », *Revue européenne des sciences sociales*, XL-123, 2002, pp. 65 -74.

⁵⁰³ BRUNETEAU Bernard, *Les Totalitarismes*, Paris, Armand Colin, mai 2014, 320 p.

retarder une société. Un calculateur électronique peut servir une administration capitaliste et une administration socialiste ; un cyclotron est un outil très efficace en temps de guerre mais il peut aussi servir en temps de paix. L'énoncé de Marx controversé selon lequel le "moulin à bras vous donnera la société avec le suzerain ; le moulin à vapeur vous donnera la société avec le capitalisme industriel", conteste cette neutralité de la technologie. Cet énoncé est modifié ensuite dans la théorie marxiste elle-même : c'est le mode social de production et non la technique qui est le facteur historique fondamental. Cependant, quand la technique devient la forme universelle de la production matérielle, elle circonscrit une culture tout entière ; elle projette une totalité historique - un "monde".»⁵⁰⁴

Si la compréhension de la technique comme discours est essentielle pour déconstruire un phénomène du langage qui s'en revendique, elle ne peut se limiter à une compréhension technophile de cette figure, particulièrement lorsque ce discours est mobilisé aux fins de sécurité. L'approche idéologique de la technique de laquelle nous nous inspirons permet d'isoler le contenu de la figure du cyberspace et de comprendre le rapport de cette fiction. Elle repose sur l'inscription de l'information dans un espace clos qui entraîne une singularité dans la perception de celle-ci. Cette impossibilité consacrée de percevoir l'information fonde son caractère sécuritaire entretenu par la réitération de figures imposées au travers d'objets techniques répétitif et de personnages conceptuels.

1 – Les « utopies » du cyberspace : la spatialisation comme représentation simplifiée et totale de l'information.

A la base du néologisme, la première idée liée au cyberspace en tant que représentation est une idée de lieu : « l'espace ». L'« espace » peut sans doute être entendu au départ dans son sens le plus communément admis d'une simple étendue physique. Cette idée d'étendue physique est à la base de nombreuses représentations du cyberspace. C'est sur ce mot précis « espace » que viendront se rattacher la plupart des disciplines quand il s'agira de parler du « cyber ». Il est vrai que l'espace renvoient à de nombreux sens variés qui le font apparaître en tant que concept : en sociologie, en philosophie, en géographie ou encore en dramaturgie [...]. Pour Raymond Aron, l'espace en tant qu'élément géographique peut être compris comme un enjeu politique, mais également comme un théâtre (abstrait) ou un milieu

⁵⁰⁴ MARCUSE Herbert (1964), 1968, op-cit. p.177.

(concret)⁵⁰⁵. La différence entre ces deux derniers sens procède essentiellement de leur rapport à une forme de nomologie. Ainsi un milieu, par exemple géologique ou climatique, se définit principalement dans un rapport de contexte objectivement mesurable. Tandis qu'un théâtre, par exemple le champ de bataille, est avant tout défini par le regard de l'observateur dans le cadre d'une activité spécifique. Chez Pierre Bourdieu, l'espace se conçoit comme une représentation du monde social destinée à mettre en valeur les phénomènes de hiérarchisation sociale⁵⁰⁶. Rattacher la vision « littéraire » de l'espace cybernétique à l'acception de ce dernier comme concept en sciences sociales semble la manière la plus simple de comprendre le terme. Cette approche ferait du cyberspace une sorte d'espace social particulier car créé par la technique et reposant sur la base d'échanges sociaux permis par elle. Le cyberspace ne serait qu'une forme abstraite de spatialisation ou de territorialité⁵⁰⁷.

« [Le cyberspace est l'] espace immatériel produit par l'ensemble des relations sociales qui s'établissent via des réseaux de télécommunication informatiques interconnectés. [...] Le cyberspace est donc une composante de l'espace parmi d'autres, qui le déterminent et qu'il détermine en retour »⁵⁰⁸

C'est autour de cette question que viennent se heurter les débats quant à la définition du cyberspace. Poser la question de la nature du cyberspace au-delà des définitions devient rapidement le terrain de conflits idéologiques plus ou moins prononcés. Si ce concept ne permet pas de saisir l'ensemble des phénomènes objets de la présente recherche, il permet néanmoins de souligner l'importance de la subjectivité des acteurs et de l'intersubjectivité qui les lient. En effet, le cyberspace est politique : le terme lui-même sert à éclairer différentes valeurs⁵⁰⁹. L'information appropriée par l'humain, n'est plus seulement un agrégat de données

⁵⁰⁵ « L'espace [géographique] peut être considéré comme milieu, théâtre, et enjeu de la politique étrangère ». Extrait du chapitre VII « De l'espace » de l'ouvrage ARON Raymond (1962), *Paix et guerre entre les nations*, Paris, Calmann-Lévy, 20 janv. 2004, 832 p.

⁵⁰⁶ « On peut représenter le monde social sous la forme d'un espace (à plusieurs dimensions) construit sur la base de principes de différenciation ou de distribution constitués par l'ensemble des propriétés agissantes dans l'univers social considéré, c'est-à-dire propres à conférer à leur détenteur de la force, du pouvoir dans cet univers. » BOURDIEU Pierre , « Espace social et genèse des classes », *Actes de la recherche en sciences sociales*, vol 52, 1984, p. 3-14.

⁵⁰⁷ Dont la dénomination variera sans cesse en fonction de l'acteur considéré : espace, dimension, environnement, champ, milieu, domaine, secteur, marché...

⁵⁰⁸ LEVY Jacques et LUSSAULT Michel, *Dictionnaire de la géographie de l'espace des sociétés*, Paris, Belin, 1033 p.

⁵⁰⁹ « valeur » s'entend ici au sens d'un principe auquel doivent se conformer les manières d'être et d'agir des acteurs.

numérisées, mais un ensemble finalisé, intégré au système de représentations de l'acteur et lié à sa recherche de vérité ou de compréhension de son environnement. Autrement dit, pour appréhender cyberspace, il faut privilégier une approche qui tienne compte des différentes subjectivités des acteurs considérés.

Sous cet angle, le cyberspace avec son impossible définition traduit malgré tout la prise en compte par l'acteur de l'enjeu des technologies de l'information comme objet de sécurité. Cette normativité « cyber » repose sur la labellisation d'un corpus technique. Autrement dit, le « cyber » est la métonymie, l'avatar de phénomènes complexes qui reposent sur la diffusion d'un corpus technologique à un grand nombre de personnes et la diffusion d'une nouvelle forme de culture de l'information. En effet, le secteur dit des technologies de l'information se distingue d'autres secteurs comme l'aviation ou l'automobile. L'informatique n'est pas un secteur économique ordinaire. D'une industrie de pointe, elle est aujourd'hui diffusée à l'ensemble des secteurs et supplante sa propre compétence à celle d'autres domaines d'expertise sur des secteurs qu'elle alimente⁵¹⁰. Cette diffusion est à nuancer quelque peu car elle reflète les fractures sociales qui déchirent la population mondiale⁵¹¹. Le cyberspace peut alors s'appréhender non plus comme un espace physique ou social ou encore un milieu mais davantage comme le marqueur discursif d'un ensemble finalisé de

⁵¹⁰ Cette prégnance de l'informatique a commencé très tôt au niveau de l'État. BAUDOT Pierre-Yves, « L'incertitude des instruments. L'informatique administrative et le changement dans l'action publique (1966-1975) », *Revue française de science politique*, Vol. 61, 2011/1, pp. 79-103.

⁵¹¹ Malgré des taux d'équipements en nette progression, l'amélioration des taux de connexion et d'utilisation dans toutes les catégories sociales, l'on constate néanmoins un écart relatif entre groupes sociaux qui n'a pas franchement évolué depuis le début des années 2000 (en fait, il reste stable). C'est le cas notamment des écarts liés à l'âge (seulement 10% des personnes au-delà de 65 ans utilisent Internet contre 68% des 16-24 ans). « Broadband access in the EU : situation at 1 July 2007 » In. *Rapport de l'Union européenne sur le haut débit*, Bruxelles, 15 Octobre 2007. Voir également : GRANJON Fabien, « La réduction de la fracture numérique », *Regards sur l'actualité*, n°327, La Documentation française, janvier 2007. Pour les chiffres bruts, voir également le site *Internet World Stats*. url : www.internetworldstats.com/stats.htm [En ligne : 1er janvier 2019].

représentations⁵¹² entendues comme des valeurs et des connaissances partagées et distincts de la somme des représentations individuelles.⁵¹³

De manière générale, si le cyberespace opère une métaphore de l'information traduite au plan géographique, il faut une nouvelle fois se méfier des idées reçues que cela engendre. Appliqué aux notions d'information et d'espace, il s'agit essentiellement pour Pierre Musso⁵¹⁴ de catégoriser une série d'idées reçues sur l'impact des technologies sur le « territoire » et le processus de révolution permanente qui semble guider les innovations en matière de technologies de l'information depuis les années 90 et qui constituent autant de fameuses « révolutions numériques ». Ainsi, Pierre Musso identifie une série de « formules miracles » qui confortent la naturalisation des technologies et la fatalité du « progrès technique » .

La première idée est celle de la réduction des déplacements par l'entremise de la technologie. Au contraire, cette mobilité s'accroît de plus en plus. Cette mobilité est aujourd'hui principalement identifiée par les notions de nomadisme numérique ou de mobilité connectée⁵¹⁵. Elle est le fruit de la diffusion de la technologie de l'information dans un nombre croissant d'objets du quotidien, le symbole étant les inventions du téléphone portable puis du *smartphone*. Dans un second temps, la déterritorialisation provoquée par le numérique s'accompagne d'une vague de reterritorialisation. Corolairement, les technologies de l'information ne provoquent pas une « indifférenciation spatiale ». Ainsi, avec l'exemple du commerce électronique, le défi est celui de la logistique qui gagne en importance. L'auteur constate une « concentration des activités et une spécialisation des territoires, une mise en

⁵¹² Typologie héritée de Durkheim qui oppose comme « réalités » sociales, les « procédés neurochimiques du cerveau », les « représentations individuelles » et les « représentations collectives ». DURKHEIM Emile, « Représentations individuelles et représentations collectives » *Revue de Métaphysique et de Morale*, tome VI, mai 1898. Les travaux de Moscovici ont enrichi et délimité la notion de représentation sociale : Construite mentalement et socialement, par et pour la pratique. La représentation y est décrite davantage comme un processus. MOSCOVICI Serge, *La Psychanalyse, son image et son public*, Paris, PUF, 1961. 512 p.

⁵¹³ Néanmoins les représentations collectives, quelque puisse être leur nom, ne sont pas proprement le marqueur d'approches subjectivistes. Le concept de représentation peut se trouver réutilisé dans différentes théories où on lui donne un rôle particulier ou une acception plus précise. Ainsi dans les approches « objectivistes », elle ne sera plus considérée comme « productrice de réalité », mais comme une simple interprétation de celle-ci. ELIAS, Nobert, *Qu'est-ce que la sociologie ?* Paris, Pocket, 1991. GASTON-GRANGER Gilles, *Sciences et réalité*, Paris, Odile Jacob, 2001.

⁵¹⁴ MUSSO Pierre, « Le Web : nouveau territoire et vieux concepts », *Annales des Mines - Réalités industrielles*, 2010/4, Novembre 2010, pp. 75-83.

⁵¹⁵ FLICHY Patrice. « L'individualisme connecté entre la technique numérique et la société », *Réseaux*, vol. n° 124, no. 2, 2004, pp. 17-51.

réseau, avec un accroissement des flux et des polarisations renforcées entre centres urbains ou innovants ». Ontologiquement, l'auteur se positionne pour un cyberespace ancré dans le réel. Selon, lui le cyberespace n'a pas à supplanter le territoire physique mais il s'additionne à ce dernier : il l'enrichit et offre de nouvelles possibilités d'interaction. Autrement dit, il « augmente » le territoire⁵¹⁶. Cette critique d'un « technicisme irénique » nous semble ainsi correspondre à l'idée de rupture épistémologique dans la construction des faits observables défendue par Jean-Claude Passeron⁵¹⁷. Cela est d'autant plus vrai lorsqu'on décrit un phénomène discursif qui par le medium du langage quitte le domaine profane pour s'infiltrer dans le champ de la connaissance. Concernant le cyberespace et ses dérivées, cette précaution est d'autant plus nécessaire que le phénomène à étudié opère une circulation très particulière.

Le cyberespace serait ainsi une sorte d'« endroit » ou tout du moins une dimension possible du social et du politique⁵¹⁸. Ce n'est pas à proprement parler une déformation du sens originel du terme puisqu'il s'agissait d'un outil de narration. Entre le cyberespace de Gibson et le cyberespace comme discours de sécurité, il y a le même potentiel d'un espace de mise en récit du comportement des acteurs. Le cyberespace n'est pas homogène, universel et dépourvu de frontières. Il est soumis à des limites physiques. Toutefois, ce caractère spatial porte également le paradoxe d'une notion dont la caractéristique majeure relève de son aspect « utopique »⁵¹⁹ à l'inverse du sens originel de ladite notion. Ce caractère utopique n'a pas vocation à englober les « discours utopistes » de certains penseurs ou hackers ou du moins qualifiés comme tels, il s'entend strictement. Il y a ici une forme de conflit de représentation

⁵¹⁶ « Le territoire augmenté (ou hyper-territoire) doit être comprise dans un sens à la fois extensif (territoire étendu) et intensif (intensification des capacités du territoire et de ses résidents). Le territoire est « augmenté » quand les capacités des personnes, des entreprises et autres institutions se trouvent amplifiées ou étendues par des ressources auxquelles on accède via le réseau : informations, outils, applications, services. » Ibid. Note n°6.

⁵¹⁷ PASSERON, 2006, op-cit. pp. 105-115.

⁵¹⁸ Cette notion d'espace est d'ailleurs étudiée avec attention par les géographes et les géopolitologues dans la mesure où elle semble déterminer toute leur appropriation de l'objet. Voir notamment BAKIS Henry, « Le « géocyberespace » revisité », *Netcom*, 21-3/4, 2007, pp. 285-296. DUPUY Gabriel, *Internet Géographie d'un réseau*, Paris, Ellipses, 2002, 160 p. ainsi que DODGE Martin et KITCHIN Rob, 2003, op-cit.

⁵¹⁹ L'utopie, au sens de Thomas More, est un lieu qui n'existe nulle part et qui manifeste la représentation d'une société idéale. Toutefois, l'utopie possède un caractère satirique et critique de la société de son auteur. Dans l'œuvre de Thomas More la société décrite recherche l'égalité parfaite et absolue de tous devant la loi en rejetant la propriété privée, le luxe, la superstition et en fondant l'organisation social sur les préceptes mathématiques. MORE Thomas, *De optimo rei publicae statu, deque nova insula Utopia*, publié en 1516. Pour l'application de la notion d'utopie au cyberespace, voir notamment MUSSO Pierre, « Le cyberespace, figure de l'utopie technologique réticulaire », *Sociologie et sociétés*, Vol. 32, n° 2, automne 2000, pp. 31 – 56.

entre un cyberespace animé d'une logique utopique et celui animé d'une logique contre-utopique.

Contrairement à l'idée reçue, le caractère utopique du cyberespace réside dans le fait que c'est un espace clos. Cet espace clos implique une capacité imposée de se connecter et de naviguer. La seconde propriété utopique du cyberespace est l'égalitarisme basé sur la soumission de chaque individu à des lois qui trouve son application principalement dans sa dimension logique au travers du code informatique. La troisième caractéristique tient à la vocation utopique du cyberespace devant s'étendre à l'ensemble du monde social afin de produire un âge d'or « la société de l'information », la « société en réseaux »⁵²⁰. Cette représentation est plus proche de la spatialisation. Le sens originel du cyberespace dans la littérature dystopique (ou contre-utopique) repose sur l'exact opposé : des temps obscurs, un cyberespace ouvert et intrusif disposant d'une emprise totale (y compris physique) sur l'humain et favorisant une répartition inégale des richesses allant jusqu'à confisquer la somme totale des connaissances humaines. Le moteur même de l'histoire vise à briser les lois de l'espace en mettant en scène des personnages qui préfigurent le hacker moderne⁵²¹. Cette représentation est plus proche du discours sur la menace.

Il y a ainsi une forme de conflit entre le discours entourant le développement des technologies de l'information et les résultats analysés au sein des corpus. L'idée d'espace vient organiser ce conflit autour d'une logique de « terre inconnue » synonyme de risques et d'opportunités. Le recours au symbole et la métaphore spatiale qui visent à décrire le cyberespace d'un point de toponymique comme un lieu exotique, un « océan » ou une « jungle » participent de cette recherche de compromis entre ces deux tendances. Le caractère utopique du cyberespace est cependant nécessaire malgré l'efficacité du discours relatif à la menace car il permet de caractériser celle-ci sans pour autant nuire au développement des technologies. La sécurité de l'information fonctionne ainsi sur ce dialogue de deux langages distincts. L'un fondamentalement sécuritaire marqué par l'utilisation du préfixe « cyber » et l'autre marqué par d'autres termes (comme par exemple le « numérique »)⁵²². Ainsi,

⁵²⁰ CASTELLS Manuel, *La société en réseaux. L'ère de l'information. Tome I*, 671 p.

⁵²¹ Cf. chapitre 1.

⁵²² Plus récemment, voir le concept de « datasphère » qui tente de dépasser une certaine forme de représentation sécuritaire : DOUZET Frédéric et DESFORGES Alix, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », *Netcom*, 32-1/2, 2018, pp. 87-108.

l'idée spatiale n'existe à première vue que dans la différenciation. L'espace cybernétique ne sert pas à décrire le milieu normal de l'acteur, au contraire, il décrit un espace où celui-ci est étranger par nature. L'idée spatiale anime ainsi une rhétorique de l'altérité qui vient décrire une complexité de l'information que l'acteur ne peut pas appréhender complètement. Autrement dit, l'espace sert à formuler une inconnue voire une incapacité de comprendre ou d'expliquer l'environnement d'un acteur. La rhétorique de l'altérité trouve à alimenter trois propriétés fondamentales du cyberespace qui permettent d'articuler les raisons de l'incompréhension qu'il implique et qui viennent nourrir l'aspect « total » de la représentation.

La première propriété est la transversalité. En tant qu'espace, l'information est transversale, elle circule en se soustrayant en partie aux limites ordinaires des sphères publiques et privées⁵²³, entre l'intérieur et l'extérieur, des frontières, des secteurs, des disciplines, des technologies, de la prévision et de la mémoire ou plus généralement des peuples. Il y a bien sur de nombreuses exceptions à ce principe et l'information possède ses propres limites. L'idée n'est pas tant une absence de limites que la remise en cause des limites traditionnelles. Cette remise en cause transforme potentiellement chaque limite en espace d'échange au travers duquel l'acteur concerné peut faire face à l'altérité qu'il s'agisse d'un particulier ou d'une organisation. L'extranéité supposée d'un certain nombre de situations implique ainsi une insistance sur les aspects transnationaux (des flux, des menaces...). La compréhension du cyberespace passe donc par une forme de compréhension aussi large que possible de l'objet.

La deuxième propriété est l'opacité. Son principe veut que la majeure partie de l'espace concerné ne soit pas accessible ou observable car dépassant la perception des acteurs du fait de leurs limites intrinsèque ou d'une « dissimulation ». Un exemple illustre bien cette caractéristique lorsque l'on parle d'Internet, c'est le « Web profond » (*deep Web*) par opposition au « Web surfacique ». Le Web profond désigne tout ce qui n'est pas accessible à travers les moteurs de recherche généralistes du fait d'une non-indexation⁵²⁴. La non-indexation peut résulter d'un contenu « non-indexable » par format, ou de contenus ne pouvant pas l'être à raison de leur caractère dynamique, non lié, de script ou de leur accès

⁵²³ Sphère publique,

⁵²⁴ Il existe également un concept de « Web opaque » qui décrit tout le contenu susceptible d'être indexé mais non-indexé. L'opacité du cyberespace ne doit pas être confondue avec ce dernier concept. Elle ne doit pas être confondu avec le « dark web » qui est illégal.

limité. L'opacité détermine principalement le caractère imprévisible de l'espace donc des menaces. Ainsi, la compréhension du sujet passe également par une compréhension aussi profonde que possible de l'objet.

La troisième caractéristique de la représentation repose principalement sur le dynamisme qui y est attaché. Ce dynamisme se comprend basiquement comme une capacité de changer au cours du temps. Ce changement est principalement le fruit des interactions complexes des acteurs. Cette dernière caractérise produit un contexte où la transversalité de l'espace décrit notamment un rapport de l'information au temps complètement distendu par rapport à la perception humaine (entre la microseconde du supercalculateur et le quasi-arrêt de la donnée morte venant alimenter les macro-données). Le sujet doté de la compréhension plus large et profonde possible doit également être capable de la faire évoluer dans un temps qui dépasse les limites de la mémoire et de la vitesse de raisonnement de raisonnement de l'humain. Transversalité, opacité, dynamisme : la plupart des traits associés à la représentation du cyberspace, y compris en dehors des aspects sécuritaires, peuvent être décrites comme les conséquences de ces propriétés du discours. Il en va de même pour la menace qui ne construit pas comme un paramètre objectif ou concret du discours. L'acteur n'est pas tant menacé qu'il n'a peur de l'être. Ces propriétés contribuent à la production d'une représentation en « singularité » de la perception des êtres humains et des organisations. S'ils ne l'ont jamais été, ces derniers ne sont plus capables de percevoir les mouvements de l'information.

2 – La sécurité, la réponse « pragmatique » à la non-maitrise de l'information.

La singularité de la perception fonde le caractère complexe de l'information⁵²⁵. Le fait de ne pas (ou ne plus) pouvoir « voir » consacre l'idée selon laquelle les utopies du cyberspace doivent susciter une forme de méfiance. Cette méfiance réside dans par la non maîtrise totale de l'évolution future des objets techniques que le cyberspace participe à définir en tant que discours. De cette manière la représentation parvient à trouver un équilibre entre les postures technophiles et technophobes, et plus encore entre ce qui relève du caractère utopique de la représentation et ce qui relève d'un pragmatisme teinté de sécurité. Si on

⁵²⁵ La complexité s'entend au sens que lui attribue Edgar Morin d'après sa lecture des travaux de William Ross Ashby, voir MORIN Edgar, *Introduction à la pensée complexe*, Paris, Seuil, coll. « Points / Essais », 2005, 158 p.

reprend l'approche de Lucien Sfez⁵²⁶, plus particulièrement sur les images, nous devrions trouver dans le cyberespace et son discours l'ensemble des marqueurs qui viennent satisfaire cet objectif et expliquer la tournure péjorative que prendra majoritairement le phénomène linguistique. Le cyberespace comme discours sur la technique opère à la fois un discours à caractère utopique et un discours pragmatique qu'il conviendra d'isoler. La synthèse de ces deux éléments est de nature à fournir l'ensemble des articulations de sécurité nécessaire à la formulation de l'association « information – sécurité » par le biais de la métaphore technicienne.

Du point de vue de l'utopie, les marqueurs sont relativement nombreux. Le premier réflexe conduit à dire que l'utopie mène à l'isolement et au déni de la réalité pour préférer une forme de vie virtuelle. Le deuxième élément combine la maîtrise du récit concernant un objet technique particulier qui vient s'inscrire dans un processus mécanique de transformation continue du monde produit par l'émergence desdits objets techniques. Le troisième niveau discours implique cette transformation du monde engendre un questionnement autour des valeurs et de la rééducation de la population (utilisatrice) aux bons usages de ces technologies (comme l'hygiène cybernétique par exemple). Enfin, le marqueur du discours utopiste articule un retour à l'état de nature par la transformation continue du monde qui constitue la dernière étape du progrès technique. Du point de vue du discours pragmatique en miroir du premier, il est important de souligner la différence produite avec l'état antérieur. Le premier marqueur est la transformation qui n'est plus un processus continu mais des ruptures introduites par l'émergence de techniques nouvelles. Il en résulte la fragmentation du peuple, une atomisation de la société qui disparaît au profit de petits ensembles. Cela implique dès lors un partage horizontal du pouvoir, la transversalité ou le « décloisonnement » des structures d'organisation. Ces éléments illustrent une forme de déclin ou de dissolution du domaine régional puisque l'État ne joue plus de rôle régulateur.

L'agencement de l'ensemble de ces éléments constitue le socle à partir duquel peut se construire un discours qui vise à transformer un objet réputé technique en objet de sécurité. C'est le cas de l'information par le cyberespace. De manière générale se retrouverons ainsi l'ensemble de discours sur le déclin de la société née de l'informatisation globale de l'ensemble de nos activités, laquelle déconstruit les liens sociaux antérieurs au profit de

⁵²⁶ SFEZ Lucien, 2002, op-cit.

nouvelles relations qui sont mobilisées dans une nouvelle culture du partage de l’information laquelle remet en cause le partage du pouvoir et l’adaptation des structures antérieures. De ce changement acté, peuvent naître deux types de discours de sécurité qui se structurent autour de l’opposition entre sécurité régaliennes et sécurité sociétale⁵²⁷.

Le premier type de discours est un discours où le sujet de la sécurité est l’individu en tant que membre de la société et en tant que consommateur. Cet individu peut être conçu comme une personne physique, ou un regroupement plus large d’individus... La cible de la menace est constituée autour de l’idée de liberté individuelle, d’identité et de vie privée auxquelles s’ajouteront une forme de pragmatisme économique centré sur l’accès à l’information la plus fiable et sur l’intérêt financier. La surveillance, la dissimulation et la tromperie y seront irrémédiablement perçue comme néfaste.

Le second type de discours sera un discours où le sujet de la sécurité est l’État comme incarnation de la société dans son ensemble. Cette notion d’État s’entend ici au sens large pour englober tout le domaine de la sécurité de l’État, y compris lorsque celui-ci sort des domaines traditionnels de la sécurité. La cible est constituée par la vulnérabilité des infrastructures, la faiblesse des mesures de protection. Le risque sera représenté comme le déclin de l’État comme régulateur ou comme le triomphe d’un ennemi abstrait (le cybercriminel, le cyberterroriste, le « hacker »...).

3 – Fétiches du discours : objets techniques répétitifs et personnages conceptuels.

Dans sa construction, la figure du cyberspace mobilise des éléments de référence pour lesquels le recours répétitif et systématique dégage une puissance répétitive qui limite par le champ de la réflexion. Ces répétitions se structurent en particulier autour de deux types de références particulières : des objets techniques⁵²⁸ et des personnages conceptuels. Les artefacts techniques sont facilement identifiables et manifestent concrètement le « cyberspace » du monde d’aujourd’hui. Les personnages conceptuels sont moins évidents à saisir, tant ils ne manifestent pas la réalité d’un cyberspace mais sont mobilisés à des fins d’argumentation⁵²⁹. A l’image du cyberspace, ce n’est pas vraiment le contenu du personnage

⁵²⁷ Cf. chapitre liminaire.

⁵²⁸ Lucien Sfez emploie le concept d’objet technique répétitif. Nous lui préfèrerons le terme « artefact ».

⁵²⁹ VENTRE Daniel, 2001, op-cit pp. 103 – 212.

qui importe mais sa capacité à convaincre du fait d'un pouvoir évocateur fort. C'est ainsi qu'il est possible de noter un tarissement des ressources théoriques et des concepts nouveaux. Plus généralement, cela entraînera une difficulté à penser l'objet au-delà d'un certain seuil de discours.

Le cyberespace mobilise plusieurs artefacts techniques particuliers pour constituer la réalité de son espace métaphorique. L'objet le plus symbolique de ce corpus est l'ordinateur (auquel s'ajoute l'ensemble de ses dérivés de l'ordinateur familial à l'ordinateur industriel⁵³⁰). Toutefois, cet objet n'est pas un ordinateur « ordinaire » car il est « connecté ». Le deuxième objet technique symbolique du cyberespace est donc Internet. Viennent ensuite tout un corpus d'objets divers qui viennent consacrer la fusion entre ces deux artefacts : téléphones intelligents ou *smartphone*, Internet des objets, informatique en nuage ou *cloud*. La particularité de ce corpus est de traduire la mobilité de l'ordinateur et d'Internet. Un positionnement du discours au niveau du flux d'informations entraînera un discours qui s'intéressera aux câbles sous-marins et la donnée (donnée personnelle, macrodonnées). Parmi, les objets inhérents à Internet trois objets auront une importance dans le discours, l'adresse IP, le courriel et le site Internet.

Les personnages conceptuels du cyberespace sont relativement nombreux. Si on exclut l'internaute et l'informaticien qui véhiculent en eux-mêmes un certains nombreux de représentations, le personnage le plus fort symboliquement au sein du discours est le « hacker ». Le hacker du discours cyberespace n'est pas un hacker de la réalité. C'est un pirate, cybercriminel, pilleur de données personnels, parfois défenseurs des libertés, parfois terroriste, espion chinois ou espion russe. Evidemment, cette caricature paranoïde n'a rien à voir avec le mouvement des hackers proprement dit. La figure du hacker est principalement grevée d'une image négative dans le discours. En tant que personne qui cherche à comprendre un système et ses règles, terme hacker possède un ensemble de significations bien plus vaste que celui de seul « pirate informatique ». Il est associé dans le discours à un auteur type des cyberattaques. Il est traditionnellement dépeint comme un individu cagoulé dans une pièce sombre en train d'examiner des codes sur son écran tout en tapant au clavier. Cette image affecte énormément le traitement du hacker dans le discours car il opèrerait de façon illégale

⁵³⁰ Ici, on pensera notamment à un système de contrôle et d'acquisition de données (*Supervisory Control And Data Acquisition SCADA*) qui a pour rôle de guider et de contrôler des installations techniques par exemple des réseaux de distribution d'eau ou d'électricité.

ou amorphe, en violation de la plupart des règles. L'activité majeure de ces personnes serait d'attaquer des systèmes et de voler des données pour elles-mêmes (bien qu'il s'agisse d'une représentation faussée). Comme le cyberspace, le terme fait l'objet de nombreuses confusions et de nombreux mythes au-delà des idées et de l'histoire de ce mouvement politique⁵³¹⁵³². Il sera possible ici de questionner la différence de représentations entre les figures du « hacker » et celle du « lanceur d'alerte ». En effet, de l'autre côté, le lanceur d'alerte est une personne qui porte connaissance d'une information à l'opinion publique qui soit susceptible de présenter un scandale, un risque, un danger à ce que cette personne considère comme contre sa représentation du « bien commun » ou « l'intérêt général »⁵³³. A l'inverse du hacker⁵³⁴, le lanceur d'alerte sera plutôt dépeint dans les corpus analysés comme une personne à protéger. Ce dernier verbe « protéger » est d'ailleurs celui qui leur est le plus associé. En termes de représentations, il y a une différence qui est fondée dans une délimitation faussée d'un rapport à l'information comprise comme connaissance.

Si le hacker représente une forme d'agresseur dans le discours de sécurité né du cyberspace. D'autres personnages conceptuels ont également une grande importance dans le discours lié au cyberspace : l'agent de l'état, le producteur de contenu et le militant⁵³⁵. L'agent de l'État est une catégorie de personnages qui regroupe le membre des services de renseignement, le militaire, l'agent de police. Les producteurs de contenu seront plutôt les journalistes, les vidéastes, et toutes les personnes travaillant dans les médias. Le militant se répartit entre les défenseurs des libertés, les patriotes et les autres porteurs d'idéologies. Que

⁵³¹ Pour un traitement du sujet de l'émergence des hackers aux États-Unis qui plonge également dans les méthodes de travail à travers l'étude de terrain du hackerspace *Noisebridge* (groupe de hackers anarchiste), voir notamment LALLEMENT Michel, *L'Âge du faire. Hacking, travail, anarchie*, Paris, Seuil, 2015, 442 p.

⁵³² Voir également BARDINI Thierry et PROULX Serge, « La culture du hack en ligne, une rupture avec les normes de modernité », *Les Cahiers du numérique*, 2002, pp. 35-54. DAGIRAL Éric. « Pirates, hackers, hacktivistes : déplacements et dilution de la frontière électronique », *Critique*, vol. 733-734, no. 6, 2008, pp. 480-495. LOVELUCK Benjamin. « Internet, une société contre l'État ? Libéralisme informationnel et économies politiques de l'auto-organisation en régime numérique », *Réseaux*, vol. 192, no. 4, 2015, pp. 235-270. Ainsi que BELLON, Anne. « Le hacker et le professeur. Mise en débat de la propriété intellectuelle sur Internet aux États-Unis », *Raisons politiques*, vol. 67, no. 3, 2017, pp. 165-183.

⁵³³ CHATEAURAYNAUD Francis et TORYN Didier, *Les sombres précurseurs : une sociologie pragmatique de l'alerte et du risque*, Paris, EHESS, 1999, 476 p.

⁵³⁴ Du point de vue statistique, lorsque l'on analyse les différents corpus (le terme n'est pas présent dans le corpus 3), le hacker se retrouve associé par le langage aux « cybercrime », « cyberterrorisme » et « cyberattaque », mais également au « djihadisme », au « terrorisme », à l'« armée ». Le hacker est ainsi dépeint comme une personne dotée de compétences utiles pour alimenter ou combattre la cybermenace.

⁵³⁵ Il existe également des personnages abstraits comme le cybercriminel, le cyberterroriste, l'adversaire, l'ennemi invisible qui ne sont pas particulièrement bien défini.

le regard porté soit positif ou négatif sur le personnage en question au sein d'un discours qui mobilise le cyberespace, il sera souvent impossible de faire face à un discours recherchant une forme d'objectivité. Si on prend l'exemple du militaire dans le cyberespace, il pourra être perçu comme un protecteur ou comme un agresseur (par exemple le militaire étranger). En cela la perception du personnage conceptuel affecte la perception du discours.

Section 3 – Une nécessaire méfiance envers les tentatives de définitions du cyberespace et des termes dérivés.

Après avoir décrit l'origine du cyberespace, avoir fait le point sur ses différents héritages et cerné quelques-unes des grandes confusions qui entourent la notion , il nous revient maintenant de faire un bref état de quelques-unes des différentes conceptualisations qui en ont été faites et d'illustrer de quelle manière elles se positionnent par rapport au discours. Ces définitions passent assez par la description d'un contenu technique toutefois leurs références aux idéaux techniques sont bel et bien présent.

En 1992, Randal Walser décrit le cyberespace comme « [...] le moyen qui donne à ses usagers le sentiment d'être corporellement transporté du monde physique ordinaire à des mondes d'imagination pure »⁵³⁶ Le cyberespace peut être l'un des concepts employés en guise de métaphore spatiale pour décrire les communautés virtuelles⁵³⁷. Dans son approche des communautés virtuelles, Howard Rheingold identifie notamment trois concepts : Le Réseau, la communauté virtuelle et le cyberespace.

« Le Réseau (avec un grand "R"), c'est le terme informel par lequel on désigne l'ensemble des réseaux d'ordinateurs interconnectés qui déploient des applications de télématique pour réunir des hommes et des femmes du monde entier dans des forums ouverts à tous. [...] Les communautés virtuelles sont des regroupements socioculturels qui émergent du réseau lorsqu'un nombre suffisant d'individus participent à ces discussions publiques pendant assez de temps en y mettant suffisamment de cœur pour que des réseaux de relations humaines se tissent au sein du cyberespace. [...] Le cyberespace, qui est un mot forgé par William Gibson dans son fameux roman de science-fiction *Neuromancien*, est le nom que

⁵³⁶ WALSER Randal, « Autodesk Cyberspace Project », *Mondo 2000*, 02, 1992, p. 264.

⁵³⁷ Voir notamment RHEINGOLD 1991 op-cit. et RHEINGOLD 1993 op-cit.

certains donnent à cet espace conceptuel où des mots, des liens affectifs, des données, de l'information et du pouvoir sont produits par ceux qui utilisent la télématique. »⁵³⁸

Le cyberespace peut être décrit comme un espace d'interaction homme-machine⁵³⁹. Lequel fournit « l'expérience d'interaction tridimensionnelle qui fournit l'illusion qu'il est à l'intérieur d'un monde plutôt qu'observer une image »⁵⁴⁰. Manuel Castells décrit la transformation des systèmes de communication de la manière suivante :

« Le nouveau système de communication transforme l'espace et le temps, dimensions fondamentales de l'expérience humaine. Les lieux perdent la substance même de leur signification culturelle, historique et géographique, pour être intégrés dans des réseaux fonctionnels produisant un espace des flux qui se substitue à l'espace des lieux. Le temps lui-même est effacé lorsque le passé, le présent et l'avenir peuvent être programmés pour interagir les uns avec les autres en un même message. ‘L'espace des flux’ et ‘le temps intemporel’ sont ainsi les fondements matériels d'une nouvelle culture, laquelle transcende et intègre la diversité des systèmes de représentation transmis par l'histoire : la culture de la virtualité réelle où le simulacre est la réalité en gestation »⁵⁴¹

Bien qu'il ne mentionne pas directement le cyberespace. Ses commentateurs y voient une définition rapprochable du cyberespace. Il faut toutefois attendre l'année 1999 pour que Martin Dodge décrive l'une des conceptions géographiques du cyberespace comme représentation des flux. Il est un espace concret et non virtuel. Et il ne possède le caractère transcendental décrit par Manuel Castells⁵⁴². La même année, David Lebreton souligne la dualité de la notion mais insiste quant-à-lui sur son caractère virtuel⁵⁴³ :

« Dédoublet la vie ordinaire, le cyberspace est un mode d'existence à part entière, porteur de langages, de cultures, d'utopies. Il développe simultanément un monde réel et imaginaire de sens et de valeurs qui n'existe qu'à travers le croisement de millions d'ordinateurs [...] Un monde où les frontières se brouillent

⁵³⁸ RHEINGOLD, 1991, introduction, traduction de l'anglais par Lionel Lumbroso en 1995.

⁵³⁹ WALKER John, « Through the Looking Glass. Beyond “User Interfaces” », In. LAUREL Brenda (ed.), *The Art of Human-Computer Interface Design*, Boston, Addison-Wesley, janvier 1990, pp. 439 - 448.

⁵⁴⁰ Ibid, notre traduction,

⁵⁴¹ CASTELLS Manuel, *La société en réseaux*, Paris, Fayard, 1996, p. 472

⁵⁴² Voir DODGE Martin, *The geographies of cyberspace*, 1999 ainsi que DODGE Martin et KITCHIN Rob, *Mapping Cyberspace*, Routledge, 2003, 280 p.

⁵⁴³ LEBRETON David, *L'adieu au corps*, Coll. Traversées, Métailié, 1999, 237 p.

et où le corps s'efface, où l'Autre existe dans l'interface de la communication, mais sans corps, sans visage, sans autre toucher que celui du clavier de l'ordinateur, sans autre regard que celui de l'écran. »⁵⁴⁴

De ces tentatives de conceptualisation, on peut déduire que le pouvoir évocateur du cyberespace est limité : le terme ne peut pas évoquer n'importe quelle idée. Il peut être difficile d'en percevoir une frontière, néanmoins l'observateur spontané saura, par le biais de son intuition, que le cyberespace recouvre plus ou moins tout ce qui est « lié aux technologies de l'information »⁵⁴⁵. Cette idée reçue doit se comprendre comme un cyberespace qui serait le « produit » informe de l'évolution et de la diffusion de la technologie des ordinateurs à une vaste population, dans de multiples secteurs sous de multiples formes. Indépendamment de l'implémentation sociale d'un corpus technique donné, comprendre les enjeux de l'information passerait exclusivement par une « approche technique ». Si cette approche confinant au dogme peut apparaître comme caricaturale, elle est souvent révélatrice.

Au travers du terme et de l'apparente opposition entre virtuel et réel, l'enjeux « cyber » interroge le statut de la technique en tant qu'objet. Ainsi que nous pourrons l'observer quand il s'agit d'analyser le discours lié au cyberespace, celui-ci semble hériter pour partie des débats liés à la compréhension et à l'étude de la technique en général. Par ailleurs, la notion suscite chez le spécialiste des sciences sociales et humaines comme chez le profane ce qui pourrait être identifié comme un « réflexe » qui consiste à invalider sa propre compétence sur des objets dits « techniques ». Il ne faudrait pas que l'on résume cet état de fait à la seule réticence des professions intellectuelles pour la(es) technique(s). Cette réticence est le résultat de la rencontre entre ce pouvoir évocateur du cyberespace et la réalité complexe que le terme recouvre. Cela le rendrait impossible à appréhender, donc à analyser, sans disposer en même temps des arcanes de la pensée technique ; lesquelles se suffisent à elles-mêmes qui puisque leur objet est supposé objectif, solide et quantifiable, et ceux malgré les enjeux humains de la sécurité de l'information⁵⁴⁶.

⁵⁴⁴ Ibid, p. 145.

⁵⁴⁵ RAUS, Rachèle, op-cit. pp 71-72.

⁵⁴⁶ Pour une synthèse desdits enjeux voir : WEBER Claude, PERROTTET Jean-Philippe, « La place de l'homme dans les enjeux de cybersécurité », Stratégique, 2017/4 (N° 117), pp. 83-98.

A – Le caractère non-souhaitable d'une définition technique du cyberspace.

Au titre des différentes sources prises en compte dans cette analyse, le cyberspace serait par exemple : « *un domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunications, des systèmes informatiques, des processeurs et des processus de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs des services en lignes.* »⁵⁴⁷ Cette définition offre cependant, en plus d'un inventaire, une dimension informationnelle et cite les opérateurs de services en lignes, sans que les termes ou les distinctions qui la compose soient particulièrement évidentes. Cette définition est celle qui est retenue en France. D'autres documents français donnent des définitions un peu différentes. Le *Livre blanc sur la Défense et la Sécurité nationale* de 2008 évoque le cyberspace comme « *constitué par le maillage de l'ensemble des réseaux.* ». Ainsi, en respectant strictement la définition, il faudrait inclure tous les réseaux dans leur ensemble. Un réseau de distribution, un réseau d'égouts, un réseau de transports peuvent ainsi être inclus dans le cyberspace.

D'autres exemples existent en dehors des documents ayant fait l'objet de l'analyse statistique. Le *Concept d'emploi des forces* de 2010⁵⁴⁸ décrit le cyberspace comme « le réseau planétaire qui relie virtuellement les activités humaines grâce à l'interconnexion des ordinateurs et permet la circulation et l'échange rapides d'informations ». Si on se limite à cette compréhension du cyberspace, on pourrait être tenté de dire que le cyberspace est Internet sans que l'intérêt d'employer un mot nouveau ne soit perceptible. Dans sa *Stratégie de la France pour la Défense et sécurité des systèmes d'information* de 2011, l'ANSSI définit le cyberspace comme « *espace de communication constitué par l'interconnexion mondiale d'équipement de traitement automatisé de données numérisées.* ». La définition de l'ANSSI traduit aussi une conception technique du cyber à travers la référence aux « *Equipement de traitement automatisé de données* », évocation des systèmes de traitement automatisé de données (ou STAD). Le STAD a été introduit en droit français par la *loi Informatique et libertés de 1978* portant notamment obligation de sécurité des données personnelles. Dans un second temps elle a été reprise par la *loi Godfrain du 5 janvier 1988* pour réprimer l'accès

⁵⁴⁷ Extrait du *Concept interarmées de Cyberdéfense* de la France. CICDE, *Concept interarmées de Cyberdéfense CIA 6-3*, juillet 2011, reprise dans les documents législatifs postérieurs analysés.

⁵⁴⁸ CICDE, *Concept d'emploi des forces*, CIA 01, janvier 2010.

frauduleux, les atteintes au système, les atteintes frauduleuses aux données ou encore les tentatives de l'un de ces délits. C'est sans doute l'un des concepts les plus flous du droit informatique. La jurisprudence de la Cour de cassation considère largement que ce concept s'applique au réseau téléphonique (France Télécom), à un réseau local entre deux machines, à un ordinateur déconnecté d'Internet, une carte bancaire...

1 – La définition du cyberespace : une information apparemment peu utile.

Peut-on comprendre le langage « cyber » sans comprendre le cyberespace ? En tout cas, la compréhension du cyberespace n'est finalement qu'une partie congrue de ce langage. Le cyberespace (avec son pluriel) représente 1,3% des résultats d'occurrences sur le corpus 1, 3,6 % sur le corpus 2, 10,8 % sur le corpus 3, 5,56% sur le corpus 4 et 3.08 % sur le corpus 5. Il serait facile de dire que cela fait du cyberespace l'une des occurrences les plus représentées parmi les groupes de faible importance. Il est également vrai que le langage « cyber » comprend d'après nos résultats entre 89,2 et 98,7% de mots différents du cyberespace. Ainsi formulée l'idée de cyberespace n'apparaît pas statistiquement pertinente comme concept sinon dans sa filiation avec les nombreux termes dérivés qui forment l'écrasante majorité des résultats.

Si le premier chapitre énonçait l'idée qu'une définition du cyberespace n'était pas particulièrement souhaitable du fait de nuit à son pouvoir évocateur. Il est possible d'affirmer qu'une telle définition est inutile voire contreproductive du point de vue des discours qu'elle cherche à expliquer. Autrement dit, le cyberespace s'analyse avant tout comme un concept sténographique qui existe d'abord parce qu'il est employé dans une variation de formes.*ad hoc* qui ne trouvent leur sens que dans un contexte et des relations aux faits spécifiques⁵⁴⁹. Le corolaire réside dans le rejet d'un débat sur la nature réelle du cyberespace au profit d'une nature exclusivement sémantique. Il n'est pas important de savoir si le cyberespace est un

⁵⁴⁹ PASSERON, 1991, op-cit.

espace, un lieu, une dimension, un « monde », un « environnement »⁵⁵⁰, un théâtre d'opération, un « substrat »⁵⁵¹, un « domaine »⁵⁵²...

2 – Idée de menace et précautions nécessaires vis-à-vis des « discours catastrophistes » à partir des années 2000.

Depuis l'introduction de l'enjeu de sécurité, l'influence de la représentation de la menace nourrit une catégorie particulière de discours qui visent une forme de prophétie d'une menace « à venir »⁵⁵³. Ces interprétations de la sécurité de l'information forment le socle d'une construction des scénarios qui envisage les pires possibilités de réalisation de la menace. Ces discours peuvent être classées entre trois grandes catégories : la cyberattaque dotée d'un impact très important, la cyberguerre, la défaillance généralisée des systèmes d'informations qui entraînerait la fin du monde. Ce discours catastrophiste correspond souvent à une reprise dans la production française de citation d'origine américaine.

La cyberattaque « majeure », c'est une attaque plus ou moins insidieuse qui viendrait endommager les systèmes d'une nation. Dans le discours, elle existe en négative de l'idée d'importance vitale attachée aux acteurs, mais également à travers l'analogie historique : « Cyber 9/11 »⁵⁵⁴, « Cyber Pearl Harbor »⁵⁵⁵. Cette attaque est différente des autres

⁵⁵⁰ HARKNETT Richard J., CALLAGHAN John 'P. et KAUFFMAN Rudi « Leaving Deterrence Behind : War-Fighting and National Cybersecurity. » *Journal of Homeland Security & Emergency Management*, Vol. 7, No 1, article 22, 2010.

⁵⁵¹ DEMCHAK Chris C, « Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World, » In. BURNS Nicholas et PRICE Jonathan (eds), *Securing Cyberspace: A New Domain for National Security*, Washington, D.C.,Aspen Institute, 2012, pp. 59 - 94.

⁵⁵² CARR Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Londres: O'Reilly, 2009, 318 p. Voir également, KEMPF Olivier, « Cyberstratégie à la française », *Revue internationale et stratégique*, 2012 n° 87, pp. 121-129. Je renverrai une nouvelle fois à l'inventaire d'épithète et qualificatif attribué au cyberspace établi par Daniel Ventre en 2011. VENTRE, 2011, op-cit.

⁵⁵³ La terminologie de discours catastrophiste pour qualifier ces définitions est empruntée à Daniel Ventre. VENTRE 2011, op-cit pp. 93 - 99. D'autres auteurs issus des théories de la guerre de l'information mobilisent le concept de chaos. Voir notamment, SCHWARTAU Winn (1994), *Information Warfare: Chaos on the Electronic Superhighway*, Thunder's Mouth Press, 1995, 432 p. ainsi que HUYGHE François-Bernard, *L'ennemi à l'ère numérique, chaos, information, domination*, Paris, PUF, Coll. Défense et défis nouveaux, 2001, 216 p.

⁵⁵⁴ Déclaration de Mike McConnell, ancien directeur de la NSA, reprise par le Sydney Monring Herald le 22 avril 2003. CANT Sue, « cyber 9/11 risk warning », *Sydney morning herald*, 22 avril 2003.

⁵⁵⁵ Déclaration de Leon Panetta, alors secrétaire américain à la défense, en octobre 2012, qui décrit une attaque informatique qui entraîne une destruction physique et des pertes de vie humaines. PANETTA Leon E., « Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City », 11 octobre 2012.

cyberattaques car elle serait tout à la fois massive, irrésistible et causerait de sérieux dommages, y compris des décès d'êtres humains.

La cyberguerre est un stade supérieur qui ne se limite pas à une seule attaque mais fait de celles-ci l'élément déclencheur d'une guerre à la fois informatique et conventionnelle. Ici encore, l'analogie historique est employée. La plus célèbre est probablement attribuée au magazine *Vanity Fair* qui concluait en 2011 que le virus Stuxnet était l'Hiroshima de la Cyberguerre⁵⁵⁶. Si le discours analysé admet que la cyberguerre nous menace, il se consacre également à dire qu'elle n'aura pas lieu. À la suite d'un article de Thomas Rid⁵⁵⁷, la cyberguerre a fait l'objet de nombreuses critiques quant à l'application du préfixe « cyber » à la guerre et au conflit armé en général. Thomas Rid met principalement en cause la représentation culturelle de la cyberguerre comme le schéma narrative évident de « forces obscures » capables de mobiliser des réseaux complexes et « arcaniques » afin de prendre les nations en otage.

L'idée de Thomas Rid est que toutes les cyberattaques ne sont qu'espionnage, subversion et sabotage (à la différence du cybercrime). La discréetion qui entoure ces cyberattaques diminue la violence politique plutôt que de l'accroître. L'auteur en retient principalement trois aspects dans la diminution de cette violence. La cyberattaque peut neutraliser sans avoir besoin de nuire physiquement à son opérateur. Le cyberespionnage peut permettre d'extraire des données sans devoir infiltrer un agent humain sur le terrain dans des opérations risquées. La subversion qui existerait aujourd'hui sous l'idée de manipulation de l'information permet d'emporter pacifiquement l'adhésion des populations. L'utilité de la cyberattaque est impactée par des contraintes affectant leurs capacités dont la principale est de pas pouvoir reproduire les bénéfices uniques de recours aux opérations humaines.

L'auteur retient trois raisons à cela : la difficulté de réussir une mobilisation uniquement avec l'informatique même s'il est plus facile de la créer, l'incapacité de l'informatique à restituer l'information dans son contexte humain afin d'en tirer des avantages politiques, idéologiques ou commerciaux (la récolte est plus facile mais demeure le problème de l'utilisation), et enfin une cyberattaque peut difficile souscrire à des visions politiques

⁵⁵⁶ GROSS Michael Joseph, « Stuxnet Worm, A Declaration of Cyber-War », *Vanity Fair*, 2 mars 2011.

⁵⁵⁷ RID Thomas, « Cyber War Will Not Take Place », *Journal of Strategic Studies*, vol. 35, n1, octobre 2011. Voir également l'ouvrage éponyme RID, Thomas, Oxford University Press, 2013, 218 p.

plus large que le sabotage. La cyberguerre telle qu'imaginée dans le discours catastrophiste n'existe pas. Toutefois, une autre « cyberguerre » existe bel et bien. Cette cyberguerre désigne l'emploi des cyberattaques sur les théâtres d'opération en plus des moyens conventionnels. « S'il n'est pas nécessaire de prévoir une cyberguerre autonome, une ligne d'opération cyber dans la planification stratégique permet aux états-majors militaires d'agir dans le cyberspace. »⁵⁵⁸ Cette dernière citation illustre le glissement du discours de la cyberguerre et du cyberconflit hors des dérivés du cyberspace vers les idées de lutte informatique (défensive/offensive).

La défaillance généralisée des systèmes d'information est consacrée par de nombreuses expressions : par exemple « cyberapocalypse »⁵⁵⁹, « cyberarmageddon » ou « cybergeddon »⁵⁶⁰. L'idée est celle d'une défaillance totale de tous les ordinateurs donc de toutes les activités qui en utilisent ; ce qui condamnerait l'humanité à retourner à l'âge de pierre (ou au moyen-âge pour les plus optimistes). Au-delà du langage, la défaillance généralisée des systèmes est également envisagée comme un risque potentiel par plusieurs organisations notamment le *World Economic Forum* qui l'a inclus dans son *global risks report* depuis l'année 2007 en que plus grave risque technologique (mais l'un des moins probables) avant qu'il ne soit remplacé par les cyberattaques (risque moins grave, mais plus probable)⁵⁶¹. Un tel événement pourrait être d'origine accidentelle mais qui aurait très probablement une origine volontaire. La défaillance généralisée des systèmes d'information repose en effet sur un effet de domino pouvant avoir comme sources une attaque, un virus, une faille d'Internet ou les limites de son expansion en termes de ressources et d'énergie⁵⁶². Ces derniers discours catastrophistes ne mettent qu'assez peu en avant l'idée de singularité technologique envisagée

⁵⁵⁸ BAUD Michel. « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique étrangère*, vol. été, no. 2, 2012, pp. 305-316.

⁵⁵⁹ L'expression « Fear of a cyber apocalypse era » est attribuée à l'ouvrage SCHELL Bernadette H., et CLEMENS Martin. *Cybercrime: a Reference Handbook*. ABC-CLIO, octobre 2004, 247 p.

⁵⁶⁰ Ces deux variantes de la même expression sont encore une fois d'origine américaine. L'expression « cybergeddon » aurait été popularisée le 6 janvier 2009 à la suite d'une déclaration de Shawn Henry, directeur adjoint de la division informatique du FBI à New-York à l'*International Conference on Cyber Security* (ICCS) (5 au 8 janvier 2009).

⁵⁶¹ Voir notamment *The Global Risks Report*, World Economic Forum, 13ème édition, 2018,

⁵⁶² L'ONG Greenpeace évaluait par exemple que le secteur des technologies de l'information représentait 1817 milliards de kWh, soit environ 7% de l'électricité mondiale en 2012. COOK Gary (dir.), *Clicking clean, who is winning race to build a green Internet?* Washington, Greenpeace, janvier 2017, 102 p.

par Vernor Vinge⁵⁶³. Cette dernière décrit l'hypothèse selon laquelle l'invention de l'intelligence artificielle viendrait détruire la civilisation humaine actuelle.

Ces discours catastrophistes viennent insister sur l'importance d'Internet en tant que ressource vitale pour la globalité de l'humanité (quand bien même il n'est pas diffusé partout). Internet devient synonyme d'un bien commun voire d'un « standard de civilisation »⁵⁶⁴ auquel tous les États devraient se conformer s'ils souhaitent rejoindre les États développés. Quand bien même ils représentent une forme d'avertissement souvent exagéré qui suppose une lecture critique, les discours catastrophistes sont une des illustrations d'une forme de dépendance aux technologies de l'information. Si la dimension technique n'est que l'un des règnes du monde social, elle sera souvent regardée comme suffisante pour comprendre les implications d'un phénomène donné sans accomplir le travail nécessaire à la compréhension de l'information et conditionne le réflexe que nous avons déjà évoqué et qui conduira l'observateur à penser qu'un problème technique aura nécessairement une solution technique...

B – Le piège de la technique et employabilité des notions dérivées du cyberespace : l'exemple de la cyberarme.

Avec la notion d'attaque (cyberattaque), la notion d'arme vient également se greffer aux débats qui entourent la sécurité de l'information⁵⁶⁵. Ceci lui est permis par l'association de la prolifération et de l'idée de menace. Cette notion a émergé dans le langage commun en 2010 avec l'affaire Stuxnet⁵⁶⁶. L'expression cyberarme peut recouvrir deux logiques complémentaires : D'une part, elle peut permettre d'envisager l'outil technique et le moyen déterminant le caractère cybérétique d'une attaque. D'autre part, elle aurait vocation à englober l'ensemble des moyens techniques, matériels et humains dédiés aux cyberattaques (comme la composante d'un système de force). C'est ainsi que la cyberarme incarne au choix

⁵⁶³ VINGE Vernor, « The coming Technological Singularity », in *Vision-21: Interdisciplinary Science and Engineering in the Era of Cyberspace*, NASA Publication, 1993, pp. 11–22

⁵⁶⁴ LINKLATER Andrew, « The ‘Standard of Civilisation’ in World Politics », *Social Character, Historical Processes*, vol. 5, 2, juillet 2016.

⁵⁶⁵ Cet exemple reprend pour partie les termes d'une analyse publiée pendant le travail de thèse dans la revue institutionnelle *Penser les ailes françaises*. AUFFRET Yves, « Existe-t-il un marché des cyber-armes ? Pour une approche critique de la notion de cyber-arme », *Penser les ailes françaises*, n°35, juillet 2015, pp 103-111.

⁵⁶⁶ DE FALCO Marco, *Stuxnet Facts Report - A Technical and Strategic Analysis*, NATO CCD COE Publications, 2012.

un ensemble détaillé de logiciels précis, ou le secteur de la cybersécurité dans son ensemble. Dans le premier cas, adopter le point de vue de la cyberarme revient à restreindre très fortement l'analyse. Dans le second cas, la notion de cyberarme n'a tout simplement plus aucun intérêt. Notons au passage la disparition de la notion d'arme défensive. S'il est labellisé « cyber », un bouclier n'est ainsi donc plus une arme. Par ailleurs, une partie de la défense contre des logiciels malveillants repose sur un ensemble de pratiques parfois qualifiées d'offensives...

Thomas Rid et Peter McBurney défendent l'idée d'une cyber-arme qui dépasse la seule composante cyber d'un conflit. Ce choix les conduit à la première solution, et à une conception très restrictive : le *weaponised software*. Si une arme désigne tout outil conçu pour menacer ou causer des dommages physiques, fonctionnels ou psychologiques à des structures, des systèmes ou des êtres vivants, alors la cyber-arme est simplement le code informatique utilisé pour des objectifs identiques⁵⁶⁷. Le niveau technologique et donc de puissance de ces « cyberarmes » fournit alors un critère pour une première typologie :

- les armes dites à faible potentiel, génériques, peu discrètes et d'acquisition facile, faciles à mettre en place et à contrer⁵⁶⁸,
- les armes à fort potentiel, spécifiques et nécessitant des investissements lourds⁵⁶⁹,
- les armes combinant des caractéristiques de ces deux catégories⁵⁷⁰,

Dans la conception de ces armes, l'accroissement du potentiel destructeur induit deux efforts : d'une part, au niveau des ressources (Temps/Recherche/Investissement) ; d'autre part, au niveau du ciblage. Ces efforts participent à la réduction du nombre des dommages collatéraux potentiels de l'arme, réduisant également son pouvoir de coercition et de menace. Tout en sachant qu'une cyber-arme dispose d'une durée limitée pour agir avant que les défenses n'évoluent suffisamment pour la contrer. L'exploitation des bugs et l'espionnage par l'intermédiaires des chevaux de Troie ne sont pas regardées comme des cyberarmes car moins

⁵⁶⁷ RID Thomas et MCBURNEY Peter, « Cyberweapons », *The RUSI Journal*, Volume 157, Issue 1, 2012.

⁵⁶⁸ Les logiciels permettant les attaques de déni de service (DDoS) par exemple ; les attaques de 2007 en Estonie sont classées dans cette catégorie. Cf. introduction

⁵⁶⁹ Notamment Stuxnet, Flame ou Gauss.

⁵⁷⁰ Certaines intrusions particulières, par exemple avec le virus I love you.

dangereux⁵⁷¹. Ils appelleraient des sanctions juridiques différentes. Le coût prohibitif des cyberarmes à fort potentiel entraîne la diminution de leur risque de prolifération, comme n'importe quel autre système d'arme. De plus en raison du degré de précision (penser pour une cible identifiée voire unique), la cyberarme dans son acception la plus restrictive devient difficilement « exportable ». De manière connexe, ceci tend à remettre en cause le postulat de la prééminence de l'attaque sur la défense. La défense est davantage présentée sous un jour favorable en raison de son coût moindre a priori, donc de sa plus grande vitesse d'évolution. Construite notamment sur le constat d'une absence de définition dans la doctrine américaine⁵⁷², cette approche s'avère intéressante pour différentes raisons. En voulant s'affranchir de la cyberguerre, Thomas Rid et Peter McBurney excluent de leur paradigme la question de l'acteur et toute la question de la défense. On retrouve bien l'intention de nuire et la perception de la menace comme conditions de l'action ou encore l'effet psychologique sur la cible. Toutefois, ce sont ici des considérations qui semblent secondaires pour les auteurs. La question de la cyberarme ne se pose pas en vertu de l'identité ou de la nature des acteurs. Corolairement, la cyberarme n'est donc pas obligatoirement régaliennne. Enfin, on assiste à un paradoxe : d'un côté ce renoncement à l'acteur s'inscrit théoriquement dans les conceptions qui font de la multiplication du nombre d'attaques un produit de la densification et de la complexification des réseaux. De l'autre côté, le recours à une cyberarme ne peut s'inscrire que dans un intérêt bien précis. Il s'agit de l'idée d'une émergence de cyberattaques raisonnées et pensées comme une réalité dont les objectifs peuvent être économiques, idéologiques et/ou militaires. Les intérêts conditionnent ainsi paradoxalement la cyberarme indépendamment (semble-t-il) de leurs propriétaires réduits à des propensions marginales. Ainsi, adopter une approche restrictive de la cyberarme conduit à décrire un ensemble précis et déterminé de logiciels malveillants. Cependant, cet ensemble non-neutre est incapable de traduire la cyberattaque dans toute sa complexité et sa variété, ignore les questions de l'exploitation des failles, du mécanisme de défense et des acteurs. De fait, la cyberarme est un point de vue inefficace qui conduira par exemple à exclure la prise en compte de l'intégralité des marchés

⁵⁷¹ L'utilisation d'un mail piégé à l'aide d'un cheval de Troie ne serait donc pas considérée comme relevant d'une cyberarme, même s'ils sont considérés comme des cyberattaques. A fortiori, l'ingénierie sociale et plus généralement les outils d'acquisition d'informations semblent ici exclus des utilisations premières de la cyberarme. Le domaine d'une cyber-arme, du point de vue de la guerre de l'information, se limiterait paradoxalement à la dégradation des systèmes avec une variation dans le potentiel de dégâts en fonction du type d'arme en cause.

⁵⁷² "Remarkably, even the US Department of Defense Dictionary of Military and Associated Terms, an authoritative 550-page compendium that defines anything from *abort* to *Zulu time*, has no definition for *weapon*, let alone for *cyber-weapon*" RID Thomas et MCBURNEY Peter, op-cit.

les plus fleurissants du secteur, notamment le marché global des technologies de sécurité informatique ou encore le marché des failles et de leurs codes d'exploitation.

Conclusions de chapitre.

Créé dans la science-fiction des années 80 à partir d'un héritage à la fois culturel et scientifique, le cyberspace est un terme qui connaît un important succès dépassant largement le cadre de l'œuvre qui l'a créé. Le caractère à la fois imprécis et fort du terme explique sans aucun doute à la fois sa popularité et la récupération de sa racine « cyber- » entraînant le phénomène linguistique « cyber » objet de cette recherche. Le cyberspace est créé dans la science-fiction à partir d'un fond commun scientifique et culturel qui emprunte beaucoup au champ de la recherche scientifique. Son sens est ensuite déformé et réapproprié pour donner lieu à une appropriation globale des technologies de l'information, d'Internet, des médias et de la robotique.

C'est sur ce socle que se construit la transformation sécuritaire de la notion dans laquelle réside notre point de départ. Il y aura donc une tendance à présenter ce « cyberspace » et la « cybersécurité » comme des objets réels à défaut de tout travail de traduction nécessaire à la recherche quelle que puisse être la discipline. De plus, le décalage sera souvent pointé entre la demande sociale autour de ce vocable et les diverses tentatives de conceptualisation. Il est facile d'observer que l'objet ainsi construit possède la force des acteurs qui le véhiculent et que cela profite d'une forme d'illusion technique autour de l'objet.

De plus, l'arlésienne de la définition technique ou scientifique d'un cyberspace qui se dérobe apparaît comme impossible à résoudre. Tant que ce piège demeure, le phénomène constitue sans aucun doute un bon concept polymorphe formé de la totalité des sens qu'il trouve au sein de chaque contexte. Mais le cyberspace, en tant que phénomène linguistique va plus loin, puisqu'il se double d'une dimension sténographique articulée par le fameux préfixe « cyber- ». La difficulté de définir le cyberspace va donc grandissante puisqu'il faudrait que cette définition survive à la multiplicité exponentielle des nouvelles formes qui émergent dans le langage. Le cyberspace constitue donc un phénomène intéressant car il interroge l'importance réciproque du langage dans la science et la place de la technique dans la société.

En effet, le problème majeur de sa définition réside dans la volonté de lui attribuer un corpus technique particulier alors qu'il n'est basiquement qu'un théâtre au pouvoir évocateur destiné à raconter des histoires. Ce pouvoir évocateur est quand-à-lui principalement tributaire de l'héritage qui est le sien : scientifique (cybernétique, cyborg) et culturel (guerre cybernétique, figure fictionnelle du cyborg). Cela entraîne de nombreuses définitions, réappropriations et confusions qu'il importe de remettre en cause. Au point de vue des confusions, il existe des confusions entre le cyberespace et l'objet technique (Internet), ainsi qu'entre le cyberespace et les autres concepts construit autour de l'idée d'information (Infosphère, sphère informationnelle). Bien qu'il ne souffre plus de confusion avec la réalité virtuelle, le cyberespace est également touché par la confusion existante entre Internet et les applications d'Internet (notamment le Web).

Si ces confusions peuvent être sources de définitions partielles du cyberespace, elles n'expliquent pas totalement le caractère partiel voire partial de certaines définitions qui viennent questionner le rapport de leurs auteurs à la technique de manière plus large. Ces définitions relèvent le plus souvent de postures technophiles ou technophobes qui ont un profond impact sur l'emploi des termes issus de ce phénomène du langage. Le sens de ce phénomène réside plus dans le contexte d'utilisation et l'objectif de ses utilisateurs, que dans un quelconque rapport à la technique. Au-delà de l'effet du langage, cela invalide a priori l'emploi technique des termes qui en sont issus ou invite à la considérer avec la plus grande méfiance. Enfin, il semble y avoir une dualité entre un sens originel du phénomène « cyber » et son évolution actuelle qui semble venir strictement le limiter à l'idée de sécurité.

L'idée sécuritaire qui grève le cyberespace semble ici tirer son origine d'une forme d'inconnu qu'il participe à décrire : la place de la technique dans la société et plus précisément celle de l'information. Construite autour d'une forme de spatialisation de celle-ci qui met en scène son caractère imperceptible, le cyberespace décrit une fiction qui devient sécuritaire et qui repose sur des mécanismes semblables à ceux que l'on retrouve dans les discours sur les techniques. Il est donc vain, voire néfaste, de rechercher une définition de celui-ci sinon pour déconstruire les outils, artefacts comme personnages, par lesquels ce discours se construit. Parvenir à une définition, si c'était possible, viendrait amoindrir la notion et son pouvoir évocateur. Cela implique donc une certaine forme de méfiance envers les propositions de définition existantes.

Ainsi ce premier chapitre aura permis de déconstruire le cyberespace dans son invention, son ambivalence et son rapport à la technique. En tant que « fiction technopolitique », le cyberespace opère dans la description métaphorique d'un espace fictif centré sur les représentations abstraites des objets techniques qui forment autant de fétiches pour alimenter un discours où la sécurité incarne une réponse pratique à une information qui dans le discours s'affranchit apparemment de toute maîtrise.

Afin de saisir le phénomène discursif dans son entier, cette approche de la notion ne suffit pas. Il faut s'intéresser aux termes qui en sont dérivés.

Chapitre 2 – Cyberespace et termes dérivés : analyse logométrique multiniveaux entre 2001 et 2016.

« Donner un sens aux statistiques requiert de recourir à des informations contextuelles recueillies de façon bien moins rigoureuse que les données statistiques elles-mêmes. [...] »

Michel GOLLAC⁵⁷³

Ce chapitre n'a pas seulement pour vocation de fournir un regard thématique sur le discours « cyber » mais davantage de regarder son contexte et son objet d'utilisation au sein de textes mis en perspectives au sein des différents corpus politico-juridiques et médiatiques. L'objectif est de déterminer les traits dominants d'un contexte d'utilisation à partir de la recherche de résultats en fréquences et cooccurrences des termes.

L'ensemble des opérations de recherche dites de logométrie a été effectué avec le logiciel libre IRaMuTeQ. Le choix s'est porté sur ce logiciel à l'issu d'une période de recherche et d'essais sur différents logiciels (Lexico 2 et 3, Hyperbase...). Construit autour de la méthode de classification dite de Reinert⁵⁷⁴, le logiciel applique une forme de classification hiérarchique descendante au corpus en misant sur les rapports de cooccurrence qui permet d'établir une classification thématique du corpus en différentes classes aussi homogènes que possibles se reposant sur les rapports de cooccurrence les plus prononcés.

Plus simplement, plus deux termes (ou « substantifs ») sont présents en même temps au sein d'un même « paragraphe » (ou « unité de contexte élémentaire » définies *ab initio*)⁵⁷⁵, plus ils ont de chance de faire partie de la même classe. Néanmoins, cet usage du logiciel ne

⁵⁷³ Propos tiré de l'ouvrage de 1964 *Method and measurement in sociology* par Aaron Victor Cicourel paraphrasé par Michel Gollac dans GOLLAC Michel, « Des chiffres insensés ? Pourquoi et comment on donne un sens aux données statistiques », *Revue française de sociologie*, n°38, 1997, p. 12

⁵⁷⁴ C'est une méthode d'analyse de données fondée sur la méthodologie « alceste » qui y apporte la notion de « mondes lexicaux » inspiré par la psychologie sociale, pour envisager la structuration de leurs cooccurrences. C'est cette notion que nous exploiterons à travers les « classes » évoquées plus avant. Voir : REINERT Max, « Les "mondes lexicaux" et leur "logique" à travers l'analyse statistique d'un corpus de récits de cauchemars », *Langage et société*, vol. 66, n°1, 1993, pp. 5 – 39. REINERT Max, « Alceste, une méthodologie d'analyse des données textuelles et une application : Aurélia, de Gérard de Nerval », *Bulletin de méthodologie sociologique*, vol. 26, n°1, 1990, pp. 24–54.

⁵⁷⁵ Ici pour plus de simplicité nous prendrons les limites de la phrases pour définir notre paragraphe à analyser.

peut pas être effectué sans un important travail sur le corpus choisi : du balisage⁵⁷⁶ *a priori*, de lemmatisation⁵⁷⁷ et de réduction *a posteriori*. Au-delà de la seule acquisition de la méthode et de la constitution des corpus, cet effort supplémentaire d'affinage implique un investissement de temps important de la part du chercheur tout en pouvant entraîner une perte de données résultant des choix opérés par ce dernier pour rendre compte des résultats. Enfin, il semble important de préciser que l'ajout du regard logométrique à notre démonstration ne saurait se substituer aux autres méthodes de collectes d'information mobilisées.

Comme souligné lors du chapitre liminaire, les cinq corpus ayant fait l'objet d'une analyse logométrique sont :

1. « *Cyber JO RF 2001-2016* » : L'ensemble des publications du journal officiel de la République française entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé. (52 textes)
2. « *Cyber JO UE 2001-2016* » : L'ensemble des publications du journal officiel de l'Union Européenne entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé. (164 textes)
3. « *Cyber DOC ONU 2001-2016* » : L'ensemble des publications du système de diffusion électronique des documents de l'ONU en français entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé. (218 textes)
4. « *Cyber Fact FR 2001-2016* » : L'ensemble des publications francophones de presse généraliste et spécialisée entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé disponibles sur la plateforme Factiva. (27957 textes)
5. « *Cyber GN FR 2001-2016* » : L'ensemble des publications francophones de presse généraliste et spécialisée entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé sur la base de données de Google News. (20362 textes)

⁵⁷⁶ Les balises de classification retenues pour notre étude sont la nature des textes, ainsi que leur année de parution/publication.

⁵⁷⁷ La simplification de toutes les formes prises par un terme conjugué, accordé, en ramenant toutes ces formes à une seule.

Inscrite dans une perspective longitudinale, la période d'étude a été fixée entre février 2001 et octobre 2016. Les cinq corpus ont été volontairement séparés en deux catégories. L'intérêt de séparer une première catégorie de corpus (1,2,3) de la seconde (4,5) réside dans deux distinctions⁵⁷⁸ : d'une part, le caractère « dépendant » ou « indépendant » de l'énoncé destiné à un « sujet immédiatement présent dans la situation d'énonciation » ou au contraire un sujet dans un contexte différent ; d'autre part, le caractère « médiatisé » du discours. Un discours lorsqu'il est médiatisé suppose que le locuteur ne s'exprime pas en son nom propre mais au nom de la fonction qu'il incarne. Cela suppose un encadrement contraignant et une restriction du thème.

La présente étude sera donc divisée entre l'analyse des discours institutionnels, l'analyse de la presse. Ces deux analyses seront ensuite complétées par une troisième section qui sera dédié à quelques-uns des éléments de discussion qui ressortent des résultats obtenus.

Section 1 – Discours « cyber » et impact normatif des enjeux sécuritaires de l'information (France, UE, ONU).

Cette première partie de l'analyse aborde principalement les corpus 1 à 3. Il s'agit de connaître des textes institutionnels prescriptifs qui emploient l'expression « cyberspace » ou un terme dérivé afin d'en cerner le contexte d'emploi à un niveau régional et international. Autrement dit, en identifiant la configuration du contexte d'emploi du phénomène discursif étudié, cette analyse cherche à tracer une fonction normative du cyberspace. Le premier corpus a été sélectionné pour constituer un miroir du terrain de la communauté cyber en France. Les deux autres (Union Européenne et ONU) ont été sélectionnés à raison de disponibilité exhaustive en langue française.

Sur chacun des corpus., cette section présentera tour à tour ses éléments constitutifs ainsi que les résultats des opérations logométriques menées à l'aide des outils statistiques sélectionnés. Un dernier temps sera réservé à une synthèse des résultats.

⁵⁷⁸ Que nous reprendrons du commentaire de *l'archéologie du savoir* de Michel Foucault réalisé par MAINGUENEAU Dominique, « Analyse du discours et archive », *Semen*, 8, 1993. Pour l'apport de cet article à une posture sociologique compréhensive du langage institutionnel : OGER Claire et OLLIVIER-YANIV Caroline, « Analyse du discours institutionnel et sociologie compréhensive : vers une anthropologie des discours institutionnels », *Mots. Les langages du politique*, 71, 2003

A – Analyse du journal officiel de la République française entre 2001 et 2016.

Corpus n°1 - Cyber JO RF 2001-2016	
« Ensemble des publications du journal officiel de la République française entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé. »	
Date de début : 1^{er} février 2001	
Date de fin : 31 octobre 2016	
Nombre de documents retenus : 52 sur 53 résultats	Nombre d'occurrences de termes « cyber » : 154 <ul style="list-style-type: none">• 2001 à 2005 (inclus) : 9• 2006 à 2010 (inclus) : 16• 2011 à 2016 (inclus) : 129

Figure 5 – Descriptif du corpus d'étude « Cyber JO RF 2001-2016 ».

Ce premier corpus (**Table 1**) est le fruit d'un travail de sélection à partir de la base de données du site Legifrance.gouv.fr⁵⁷⁹. Son bornage chronologique a été réalisé à partir des premiers résultats identifiés jusqu'au 31 octobre 2016 afin de permettre le traitement de ces données dans le temps de la thèse. Sur cette période de 15 ans, 8 mois et 30 jours, c'est un ensemble de 52 documents⁵⁸⁰ contenant au moins une occurrence du mot cyberspace ou l'un de ses dérivés dont la publication au journal officiel a été reportée dans la base de données⁵⁸¹. Si le degré de fiabilité de ces données semble peu discutable, il faut néanmoins souligner deux limites dans la base de données. D'une part, la base de données de référence se limite au plus haut niveau de la hiérarchie des normes juridiques. D'autre part, la base de données se limite

⁵⁷⁹ Base de données publique LEGI, contenant le texte intégral de la législation et de la réglementation nationale françaises. Ces données sont fournies par la Direction légale de l'information administrative (DILA) et sont réutilisables gratuitement sous licence ouverte. Pour cette recherche c'est la version texte qui a été utilisée et qui couvre la période 1990 à nos jours. Lors du traitement, les données à caractère personnel de la base de données ont été exclues.

⁵⁸⁰ Le moteur de recherche a identifié 53 résultats, mais un même texte y avait été cité deux fois (la version non-consolidée de la *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*)

⁵⁸¹ Le total de ce premier corpus est évalué à 412 791 mots, soit environ 1163 pages de texte.

essentiellement au droit en vigueur. Autrement dit, cette recherche est cantonnée au plus haut niveau de l'État et ne tient pas compte de l'ensemble des décisions administratives et actes non-décissoires pris par les collectivités, les autorités judiciaires, ou les services déconcentrés de l'État. Elle ne tient pas compte non plus d'anciens textes qui auraient potentiellement souscrit à la règle de discrimination du corpus, mais qui aurait disparu du droit positif suivant le cours normal de la vie juridique.

Toutefois, cette limitation est à nuancer. En effet, si la présence du terme cyberspace dans le langage n'est pas si ancienne, cette double discrimination supplémentaire permet de ne pas tenir compte des textes dont l'impact est limité à une échelle locale ou dont l'impact aura été limité vis-à-vis des usages principaux de notre objet discursif qui constituent la finalité de la présente analyse. L'intégration des documents dans le corpus a été effectuée en tenant compte de leur nature et de leur date de signature. L'ensemble documentaire a été nettoyé de sa mise en forme (tableaux, listes...) et redécoupé en segments. Tels des paragraphes, ces segments ont été construit sur un critère de taille relatif au nombre d'occurrences qu'ils contiennent. Afin de mener à bien notre traitement par cooccurrence, le paraphe au sens de cette analyse s'entend donc comme un segment de 7 substantifs⁵⁸². Un dictionnaire d'expression a été utilisé afin de limiter les problèmes concernant les mots composés.

Au cours de cette étude, plusieurs types d'opérations ont été menées sur le corpus :

1. Le recensement de toutes les occurrences du terme cyberspace et des termes dérivés (**Figure n° 5**).
2. L'agrégation dans un sous-corpus de l'ensemble des segments de textes concernés par la première opération.
3. Une classification hiérarchique descendante (chi 2) (**Figures n° 6 et 7**).
4. Une analyse de similitude fondée sur les cooccurrences sans et avec la prise en compte l'affixe « cyber » (**Figures n° 8 et 9**).

⁵⁸² Nous avons repris le nombre conseillé par Magali Guaresi dans son étude thématique des discours de candidature à la députation. Le logiciel employé utilise par défaut des segments de 40 items. Ce qui considérant notre mode de construction de ces segments est beaucoup trop important pour avoir une analyse suffisamment fine lors de certaines opérations (notamment la classification hiérarchique descendante) GUARESI Magali, « Les thèmes dans le discours électoral de candidature à la députation sous la Cinquième République. » op-cit.

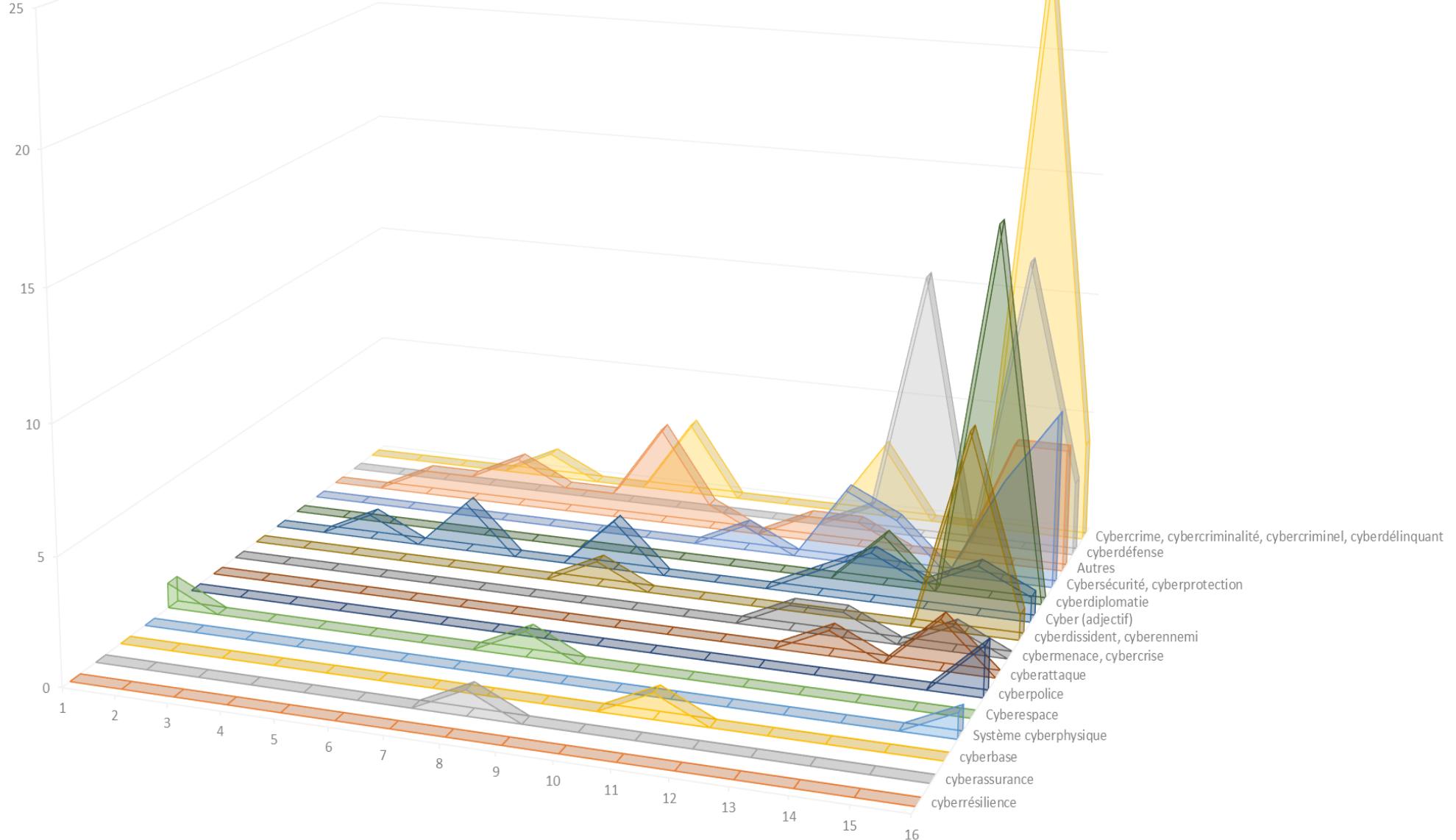


Figure 6 – Recensement des occurrences des termes « cyber ». Corpus n°1

1 – Analyse des résultats du recensement (Corpus 1).

Le recensement des occurrences des termes « cyber » (Figure 5) montre que, lorsqu'un terme « cyber » est employé, c'est en tant affixe pour des termes issus des variations autour de la cybercriminalité, la cyberdiplomatie ou de la cyberdéfense et plus généralement de la cybersécurité⁵⁸³. Si le cyberspace fait partie des occurrences les plus anciennes et ressurgit de temps en à autre au gré des publications, force est de reconnaître que le terme originel est bien moins usité que ces nouvelles compréhensions. Ce dernier champ lexical semble ici démarquer une première fois en 2008 et commence à prendre de l'importance dans l'année qui suivent. La période de 2012 à 2014 marque ici un accroissement de cette tendance et semble consacrer une utilisation du cyberspace pour parler de question de sécurité. C'est également cette dimension à laquelle se réfère dans les textes le qualificatif « cyber » utilisé pour qualifier tantôt des situations de « dématérialisation » d'un certain nombre d'activités et de service, tantôt des situations où ce volet numérique des activités humaine vient poser une question de sécurité⁵⁸⁴. Des nuances doivent être apportées. Avec 154 occurrences pour 52 textes, le cyberspace ou ses dérivés n'apparaissent jamais comme le thème principal des textes du corpus. C'est tout au plus un thème secondaire. Par ailleurs, sur une période d'une quinzaine années, 83.77% des résultats interviennent après 2010. Les plus grandes années étant 2013 (19 occurrences), 2016 (24 occurrences) et 2015 (73 occurrences). Ces trois années représentent à elles seules 116 occurrences, soit 75.32% de celles comprises dans ce corpus (Figures 5 et 6)⁵⁸⁵. Une autre nuance à ces résultats est caractérisée par la présence de quelques termes divers, notamment le cybercafé, ou le cyberdéveloppement qui ne sont pas spécifiquement associé à un discours de sécurité au sens classique du terme encore qu'ils fassent l'objet d'un usage associé à l'idée de liberté sur lequel nous aurons l'occasion de revenir... Du point de vue des résultats obtenus, le cyberspace et les termes qui y sont associés existent non pas seulement comme le marqueur d'une numérisation d'activités ou de service mais comme enjeux de sécurité. Le discours

⁵⁸³ Les désignations des courbes recoupent diverses variations des énoncés (ex de cyberdiplomatie : cyberdiplomatie·s, cyberdiplomate·s, cyberambassadeur·s, cyberdiplomatique, cyberdiplomacy...).

⁵⁸⁴ Dans le classement, certaines occurrences ont néanmoins été traitées comme des occurrences ordinaires en fonction de leur sens. Par exemple, une occurrence de « crise cyber » sera comptabilisée comme « cybercrise » tandis que l'offre « cyber » de tel ou tel industriel sera comptée à part car le « cyber » devient un secteur proprement dit.

⁵⁸⁵ Classement des séries d'occurrences par année : 2013 (Cyberdéfense – Cybersécurité [...] – Cyberdiplomatie – Cyber (adj)), 2015 (Cybersécurité [...] – Cyberdiplomatie – Cyberdéfense), 2016 (Cybersécurité [...] – Autres – Cybercrime [...]),

correspond ici, soit à l'évocation d'un enjeu ou d'un secteur, soit à une description d'une fonction pour un organisme ou l'un de ses membres. D'aucuns souligneront ainsi la faiblesse de cette notion. Les termes analysés ne forment aucune catégorie à proprement parlé : ils décrivent des objets très différents en termes de nature ou de secteur. Ils mettent ainsi l'observateur devant une hétérogénéité telle que celui-ci serait tenté de recourir au « concept sténographique » pour décrire le cyberespace malgré la référence à l'idée de sécurité. C'est un nouvel élément qui vient rajouter à l'idée que le cyberespace ne peut se comprendre dans l'ensemble de ses variations en écartant le contexte de son emploi. La faiblesse apparente de la notion de cyberespace se nourrit également de la nature des documents présents : seulement deux lois sur 52 textes en plus de 15 ans. Par ailleurs, deux lois propres au secteur de la défense⁵⁸⁶. Or, malgré ce fait, c'est le cybercrime et ses variations qui sont le thème le plus présent au sein du corpus. Tandis qu'en marge se développe également le lexique de la cyberdiplomatie. Par ailleurs, de nombreux textes du corpus concernent la vie de l'administration en général ou la vie non-institutionnelle. Il n'y a donc pas particulièrement de secteur dédié mais une forme de partage des activités au sein des différents secteurs concernés par les publications du corpus. Si les résultats obtenus indiquent un accroissement des constructions et des usages sécuritaires des termes liés au cyberespace, intrinsèquement ils ne permettent pas de mettre en avant un phénomène de révolution brutale dans le langage. Les thèmes de la cybersécurité et du cybercrime sont présents depuis 2002. Seule la prise en compte d'une forme de diplomatie numérique avec la cyberdiplomatie semble illustrer un changement de terme. Au niveau des occurrences secondaires, il faut constater de manière transversale que les références à l'acteur (cyberdissident [...], cybercriminel...) sont plus nombreuses que les références au risque et à l'attaque dans la désignation du problème de sécurité de l'information. Loin de conduire une réelle transformation de sens, le discours « cyber » vient ici appuyer une série de désignations de l'adversaire traditionnelles : l'ennemi, le dissident, le terroriste, le criminel... Le terme auquel la publication a recours est alors synonyme de moyens nouveaux pour des phénomènes anciens. Ce dernier principe vaut également assez souvent pour le diplomate ainsi que pour la police ou l'entreprise. Les moyens désignés sont essentiellement liés à l'informatique, Internet et leurs applications.

⁵⁸⁶ Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale et la Loi n° 2015-917 du 28 juillet 2015 actualisant la programmation militaire pour les années 2015 à 2019 et portant diverses dispositions concernant la défense.

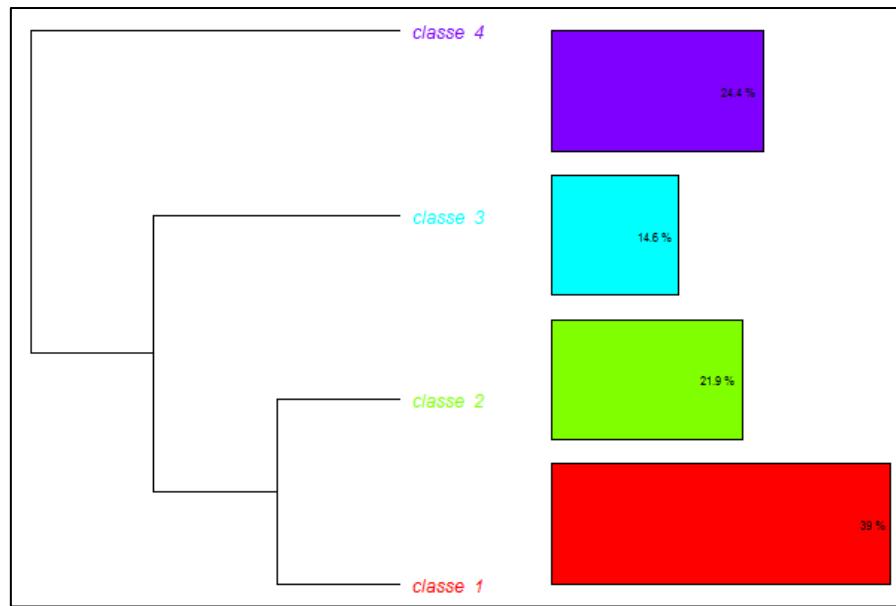


Figure 7 – Chi 2 - Formes les plus représentatives de chaque classe. Corpus n°1

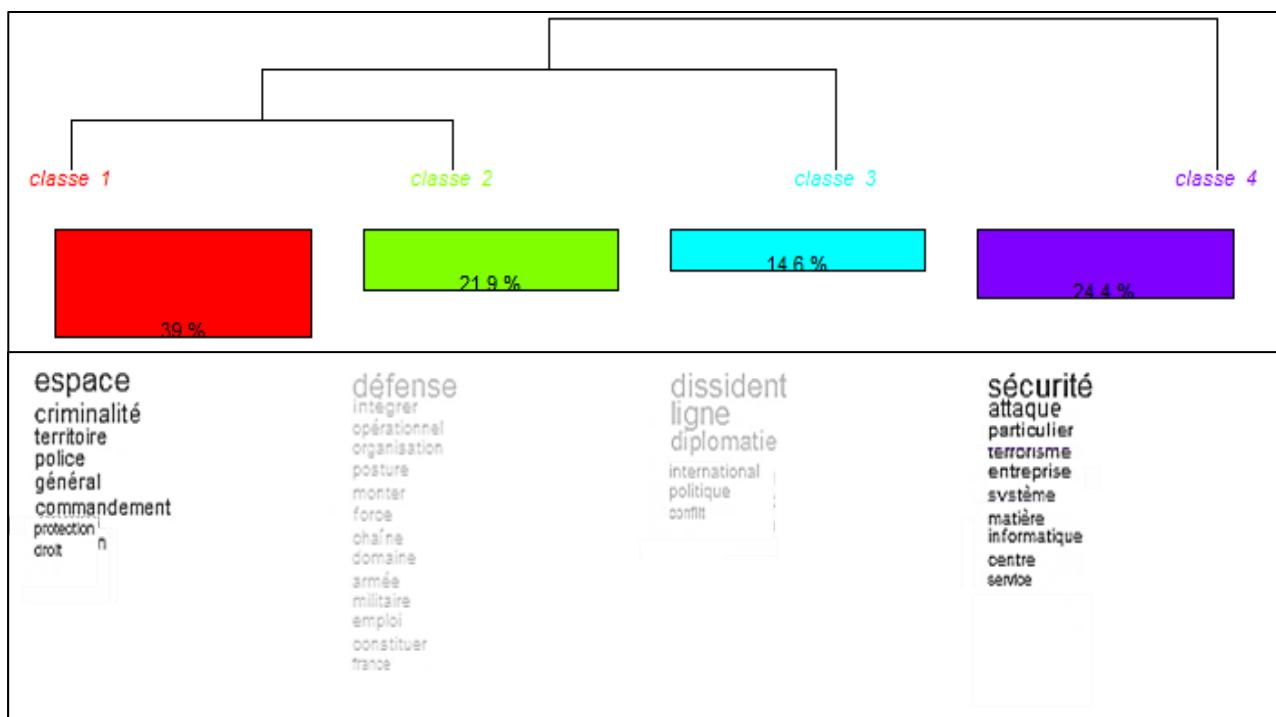


Figure 8 – Chi2 - Classification hiérarchique descendante des segments « cyber ». Corpus n°1

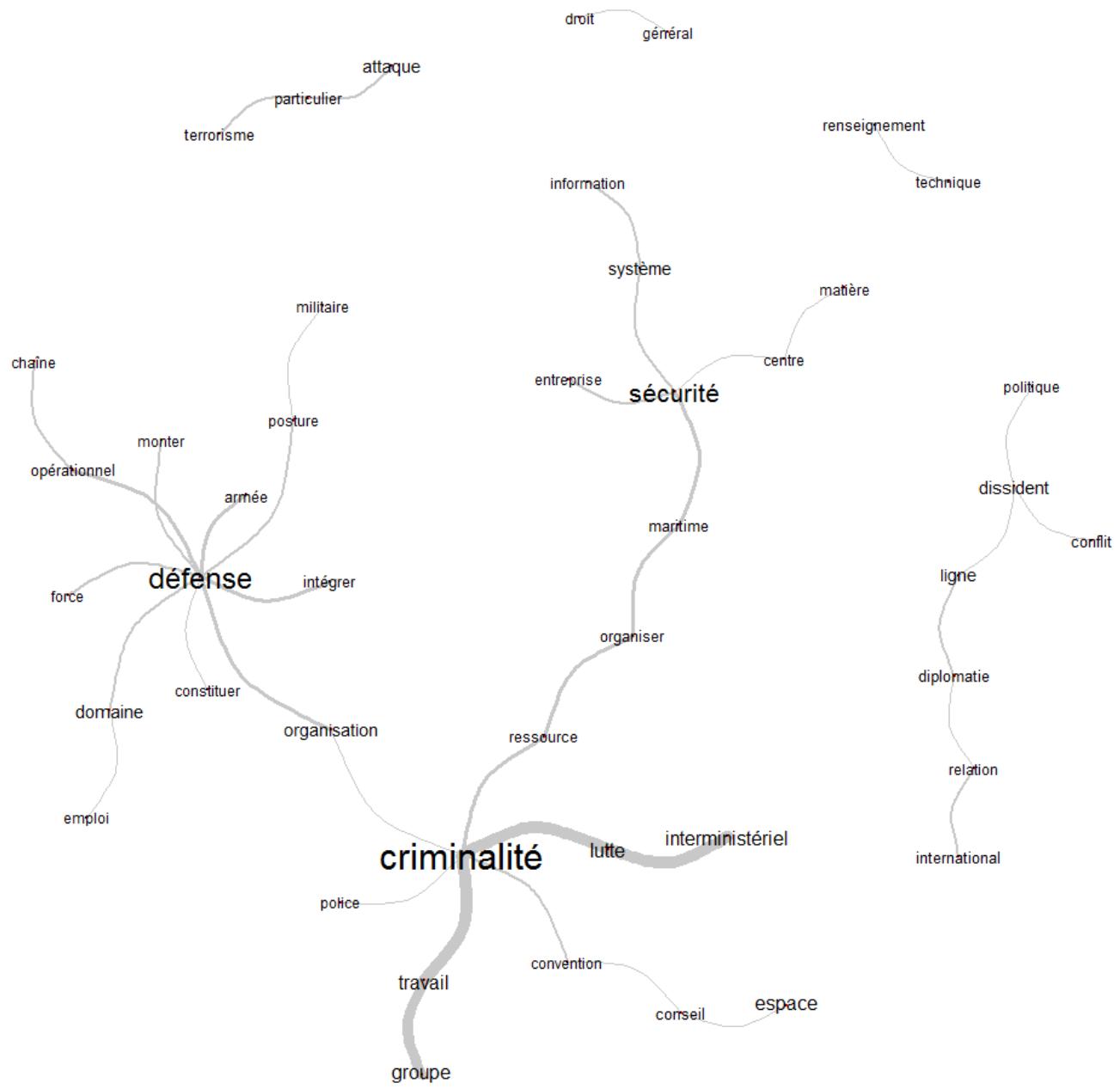


Figure 9 – Analyse de similitude en l'absence des termes « cyber ». Corpus n°1

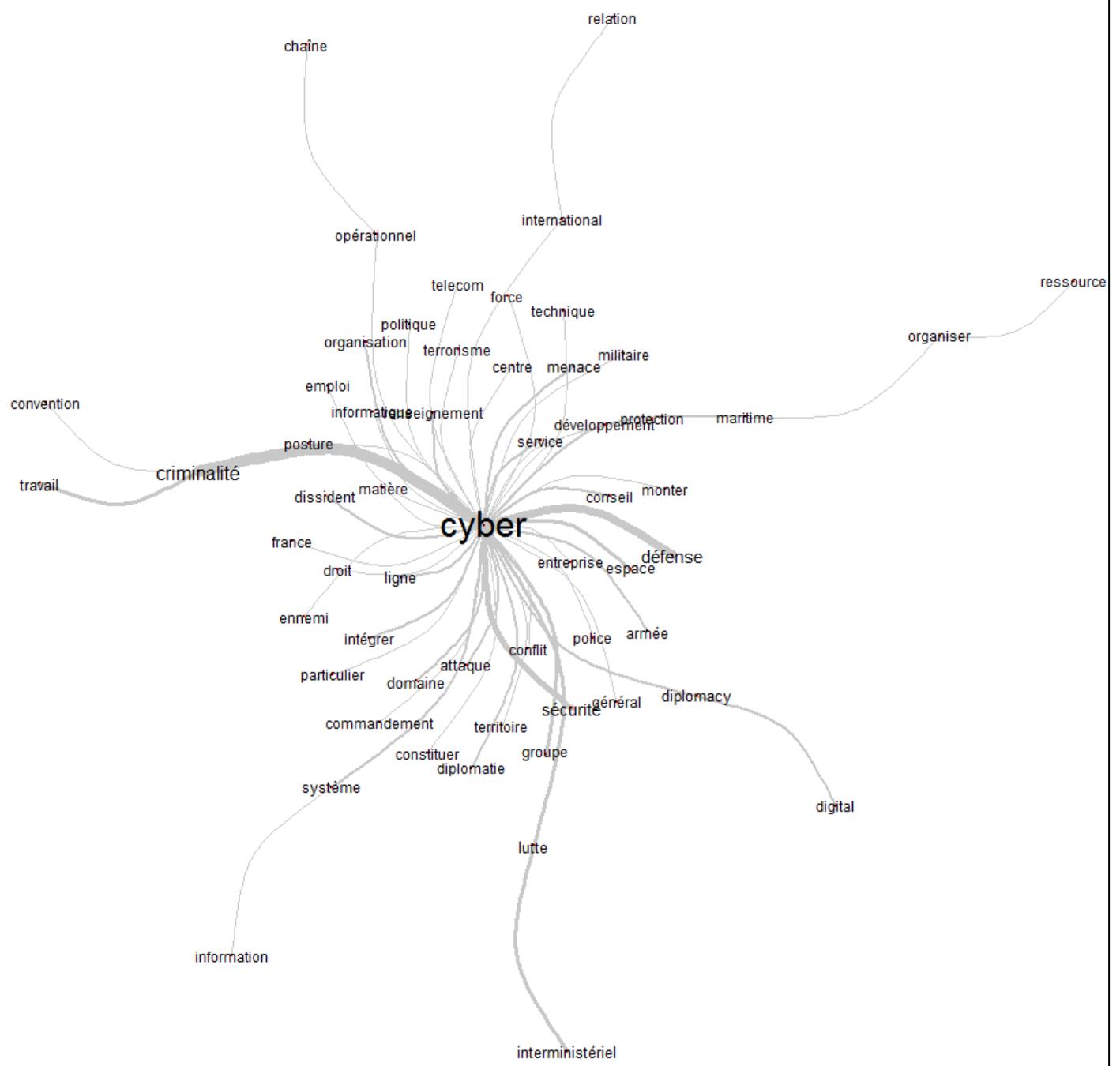


Figure 10 – Analyse de similitude des termes « cyber ». Corpus n°1

2 – Résultats des approches thématiques : mondes lexicaux et analyse de similitude (Corpus 1).

Cette sous-section vise deux types de résultats : d'une part, ceux de la classification hiérarchique descendante sur le corpus 1 (**Figures 6 et 7**), et d'autre part, ceux des analyses de similitudes sur le même corpus (**Figures 9 et 10**). Pour rappel, ces analyses se fondent non plus sur l'occurrence mais sur leurs cooccurrences ce qui permet de voir émerger des pôles du discours.⁵⁸⁷ Par ailleurs, ces dernières analyses se focalisent sur l'utilisation de l'affixe « cyber » plutôt que sur les variations des termes composé.

La classification hiérarchique descendante⁵⁸⁸ a abouti sur ce corpus à 4 classes (**Figures 6 et 7**) :

- La classe 1 (39% du corpus) qui concerne essentiellement l'inscription du cyberspace dans la vie institutionnelle, dont les substantifs les plus représentés sont : « espace », « criminalité », « territoire », « police », ...
- La classe 2 (21,9% du corpus) qui touche aux aspects Défense du cyberspace, dont les substantifs les plus représentés sont : « défense », « intégrer », « opérationnel », « organisation », ...
- La classe 3 (14,6% du corpus) qui relève de la dimension diplomatique, avec : « dissident », « ligne », « diplomatie », « international », ...
- Et classe 4 (24,4% du corpus) qui concerne plus spécifiquement la cybersécurité en elle-même et qui comprend : « sécurité », « attaque », « particulier », « terrorisme », lequel arrive à égalité avec « l'entreprise » ...

La hiérarchie entre les classes a également son importance, on constatera que les classes 1 et 2 sont associées (60,9% du corpus) et mises en parallèle de la classe 3, avant d'être reliées à la classe 4. Il est possible d'en déduire qu'il existe une forme d'accord de sens largement majoritaire entre un premier monde lexical où la spatialisation du cyberspace aboutit à la prise

⁵⁸⁷ Cf. cadre théorique des analyses de discours (introduction)

⁵⁸⁸ La classification est menée sur deux tableaux dans lesquels les lignes ne sont plus des segments de texte ou des unités de contexte élémentaire mais des regroupements de segments de texte comprise comme l'unité de contexte. Le même traitement est ainsi fait deux fois, mais en changeant le nombre de formes actives par unité de contexte.

en compte de la criminalité comme enjeux principal avec l'intégration du cyberspace dans l'environnement de la défense nationale et ses opérations. En face de ce consensus, le domaine de la diplomatie apparaît un peu en décalage et défend une vision qui si elle demeure portée sur la sécurité raisonne avec un langage différent et d'autres préoccupations. Il est sans doute opportun de constater que s'opposent ainsi deux visions tournées vers l'échelon national comme cadre de vie avec la vision tournée vers les échanges interétatiques. A l'échelle de la France, nous pouvons établir un lien avec la vision du cyberspace régaliennes de l'administration dans toutes ses composantes. Même si la nuance demeure notamment avec la présence du terrorisme, c'est également pour cette raison que le particulier et l'entreprise ne se retrouvent que dans la classe 4 (**Figure 8**). Ces résultats sont en partie confirmés avec les analyses de similitudes (**Figures 9 et 10**)⁵⁸⁹. Également fondées sur les cooccurrences, mais avec un système de classification un peu différentes, les opérations conduites aboutissent à quelques variations dans les résultats qui viennent nuancer les conclusions de la classification hiérarchique descendante et aboutissent à une cartographie différente des substantifs à partir des mêmes données et du même indice de calcul. Les différences sont essentiellement les suivantes : les trois idées majeures que sont la « criminalité », la « défense » et la « sécurité » qui forment les éléments les plus représentés dans ces analyses (**Figure 9**). Cette dynamique est accentuée quand on examine la situation à partir de l'affixe « cyber » (**Figure 10**) avec l'adjonction d'autres liens entre le « cyber » et « informatique », « service », « domaine », « espace », « protection » et « menace ». Se retrouve également un ensemble consacré à la diplomatie ainsi que l'existence de petits ensembles secondaires qui avaient été fondus avec les plus grands dans la première analyse (droit, terrorisme, renseignement) qui n'appartiennent pas à proprement parlé à l'une des grandes catégories. Pour tester dans une conception fonctionnelle de l'objet « cyber » en tant que discours, les liens principaux entre les grands ensembles (on ne peut plus parler à ce stade de hiérarchie) sont marqués par des cooccurrences qui se construisent à partir d'un vocabulaire propre aux organisations (organiser, organisation, ressource). Cette importance de la structure et du fonctionnement vaut également pour la hiérarchisation à l'intérieur de chacun des thèmes : la « criminalité » est reliée à l'idée de « groupe » de « travail » et de « lutte » elle-

⁵⁸⁹ Analyse qui produit des graphes à partir de la librairie « igraph » de R. Le tableau en entrée est un tableau de présence / absence. La matrice de similitude est calculée à partir de l'indice de cooccurrences des termes (avec un seuil minimal fixé empiriquement à 5 pour la lisibilité des résultats). Le mode de présentation des données retenu est celui dit de « Fruchterman Reingold ». Cf. FRUCHTERMAN Thomas .M.J. et REINGOLD, Edward.M. « Graph Drawing by Force-directed Placement », *Software - Practice and Experience*, 21, 1991. La taille du texte et l'épaisseur des traits indiquent en relatif l'importance des occurrences du terme ainsi que la force des relations de cooccurrences qu'il entretient avec les autres éléments du corpus.

même portée à un niveau « interministériel ». La « défense » est reliée prioritairement à « armée », « opérationnel » et à « organisation ». De son côté, la « sécurité » est reliée à « entreprise » et « système ».

B – Analyse du journal officiel de l’Union Européenne en français entre 2001 et 2016.

Corpus n°2 - Cyber JO EU 2001-2016	
« Ensemble des publications du journal officiel de l’Union Européenne en français entre 2001 et 2016 contenant le mot cyberespace ou un terme dérivé. »	
Date de début : 1^{er} février 2001	
Date de fin : 31 octobre 2016	
Nombre de documents retenus : 164 sur 289 résultats	Nombre d’occurrences de termes « cyber » : 2743 <ul style="list-style-type: none">• 2001 à 2005 (inclus) : 161• 2006 à 2010 (inclus) : 139• 2011 à 2016 (inclus) : 2443

Figure 11 – Descriptif du corpus d’étude « Cyber JO UE 2001-2016 ».

Ce second corpus (**Figure 11**) est le fruit d’un travail de sélection à partir de la base de données du site Eur-lex.europa.eu⁵⁹⁰. La période d’analyse est identique à celle du précédent corpus. Si 289 résultats ont été identifiés pour notre recherche, seuls 164 ont été retenus pour cette analyse⁵⁹¹. Les raisons ayant pu conduire à l’exclusion sont au nombre de trois : soit, le document comportait comme seule mention un nom propre (ou le nom d’un lieu), soit il s’agissait d’une version consolidée d’un texte antérieur qui venait réitérer quasiment l’ensemble

⁵⁹⁰ La base de données EUR-LEX comprend les textes produits principalement par les institutions de l’Union européenne, mais aussi par des États membres dans le cadre de l’organisation. Sauf indication contraire, la réutilisation, à des fins commerciales ou non, de données provenant du site web EUR-Lex est autorisée moyennant mention de la source (« © Union européenne, <http://eur-lex.europa.eu/>, 1998-2017 »).

⁵⁹¹ Soit un corpus de plus de 8 millions et demi de mots.

des données précédemment incorporées dans le corpus⁵⁹². Ce dernier type de documents était assez présent, ce qui a retardé la recherche, mais a permis une diminution de la base donnée par l'exclusion d'une partie des résultats et une accélération du traitement des données. La spécificité de ce corpus par rapport au premier réside dans la richesse du type de documents et dans leur taille. D'une part, le journal officiel de l'union européenne prend en compte une grande variété de document allant des sources de droit dérivé des traités (Règlements, directives, décisions) mais aussi des documents de travail et de nombreux avis sur divers projets. C'est sans doute la raison pour laquelle, il y a de nombreux documents sur les mêmes sujets et qui favorise une polarisation plus forte des thèmes que dans les corpus 1 et 3. D'autre part, les documents de l'union européenne sont souvent très longs⁵⁹³. Cela induit également des effets d'échelle sur les résultats sur le recensement des occurrences et l'analyse de similitudes dont il faut rendre compte avec un niveau détail moins avancé afin de pouvoir conserver leur lisibilité⁵⁹⁴. A nouveau, l'intégration des documents dans le corpus a été effectuée en tenant compte de leur nature et de leur date de signature. L'ensemble documentaire a été nettoyé de sa mise en forme (tableaux, listes...) et redécoupé en segments. Les opérations conduites sont sensiblement les mêmes que pour le corpus n°1 :

1. Le recensement de toutes les occurrences du terme cyberspace et des termes dérivés (**Figure 12**).
2. L'agrégation dans un sous-corpus de l'ensemble des segments de textes concernés par la première opération.
3. Une classification hiérarchique descendante (chi 2) (**Figures 13 et 14**).
4. Une analyse de similitude fondées sur les cooccurrences sans et avec la prise en compte de l'affixe « cyber » (**Figures n° 15 et 16**).

⁵⁹² Comme pour le Journal Officiel de la République Française, les arbitrages ont été conduits en faveur des versions les plus récentes des textes lorsque c'était possible.

⁵⁹³ Alors qu'elle ne constitue pas la base de données qui comprend le plus de documents juridiques de ce corpus, elle est de loin la plus imposante en volume. Une comparaison simple à établir serait la suivante : alors que la base de données de l'ONU est environ un tiers plus grand que celle de l'Union Européenne en termes de nombre de documents, cette dernière est deux fois plus lourde que sa pendante de l'ONU (format .txt). Au titre d'anecdote, la base de données du Corpus 2 fait plus 8 millions et demi de mots, et plus de 41000 pages sur le logiciel *Microsoft Word* (Police « Courrier new », 10.5, interligne simple), ce qui dépasse la limite de ce dernier logiciel qui ne peut donc pas l'ouvrir (conclusion à laquelle il arrive après environ 2h30 de comptage des pages sur station de travail dotée d'un processeur *Intel core I7* et de 16 giga-octets de mémoire vive).

⁵⁹⁴ Cf. infra.

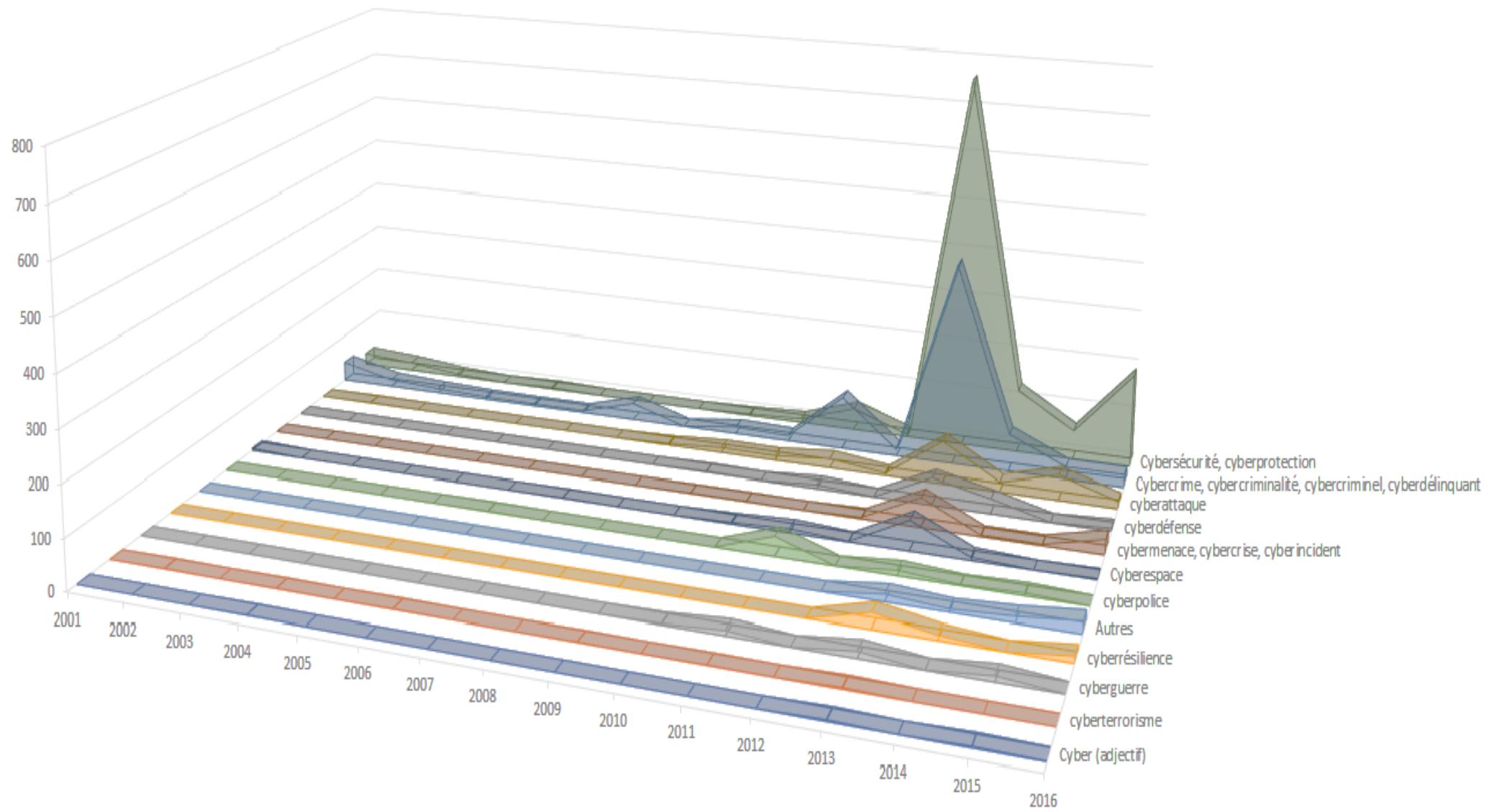


Figure 12 – Recensement des occurrences des termes « cyber ». Corpus n°2

1 – Analyse des résultats du recensement (Corpus 2).

Par rapport au premier corpus, le recensement des occurrences des termes « cyber » (**Figure 12**) montre que, lorsqu'un terme « cyber » est employé, c'est en tant affixe pour des termes issus des variations autour de la « cybercriminalité » ou de la « cybersécurité »⁵⁹⁵. Les autres variations autour des termes semblent relever ici du secondaire. Si on prend les premières catégories dans l'ordre : « Cybersécurité », on trouve 1251 occurrences (c'est presque la moitié des occurrences du corpus 2. Cf. **Figure 11**). La cybercriminalité arrive en deuxième position avec 797 occurrences. Les trois termes suivants que sont « cybermenace », « cyberdéfense », et « cyberattaque » obtiennent respectivement 85, 100 et 101 occurrences. Il y a donc des fossés entre le premier et le second terme, puis entre ces deux premiers termes et les suivants. Si le « cyberespace » fait à nouveau partie des occurrences les plus anciennes⁵⁹⁶ et ressurgit de temps en à autre au gré des publications, il trouve ici une utilisation particulière car il est souvent employé dans un contexte touchant aux libertés publiques, plutôt que des aspects liés plus directement à la sécurité de l'information où lui sera préféré les termes de « cybersécurité » et de « cyberprotection ». Sur une période d'une quinzaine années, 91.33 % des résultats interviennent après 2010, avec une considération particulière pour l'année 2013 qui mobilise à elle-seule 54.42% de l'ensemble des occurrences du corpus avec 1508 occurrences (dont un peu plus de la moitié d'occurrence du groupe de variations « cybersécurité »). A côté de cet effet majoritaire, il faut souligner à nouveau la préoccupation plus importante des textes pour les questions de criminalité que de défense. Il y a en revanche un véritable écrasement de l'usage de l'affixe « cyber » comme épithète ainsi qu'une baisse des autres termes tels « cybercafé » ou « cyberdéveloppement » qui ne représentent plus que 0.54% des occurrences⁵⁹⁷. D'après les résultats, l'utilisation du « cyber » en tant que désignation d'un secteur de la sécurité de l'information est également en baisse et semble incarner ici un idiome à la française qui n'est pas reconduit au-delà des frontières, y compris dans les autres États francophones européens. Les résultats mettent également en avant une meilleure prise en compte de l'idée résilience des systèmes dans les normes juridiques au niveau européen. Bien que depuis une période

⁵⁹⁵ Les désignations des courbes recoupent diverses variations des énoncés. Cf. Corpus n°1.

⁵⁹⁶ 4 occurrences en 2001.

⁵⁹⁷ Contre 14.94% du corpus 1 et 9,2% du corpus 3.

particulièrement récente, ce dernier thème semble trouver un écho plus important au sein de la communauté française dans le champ scientifique notamment.

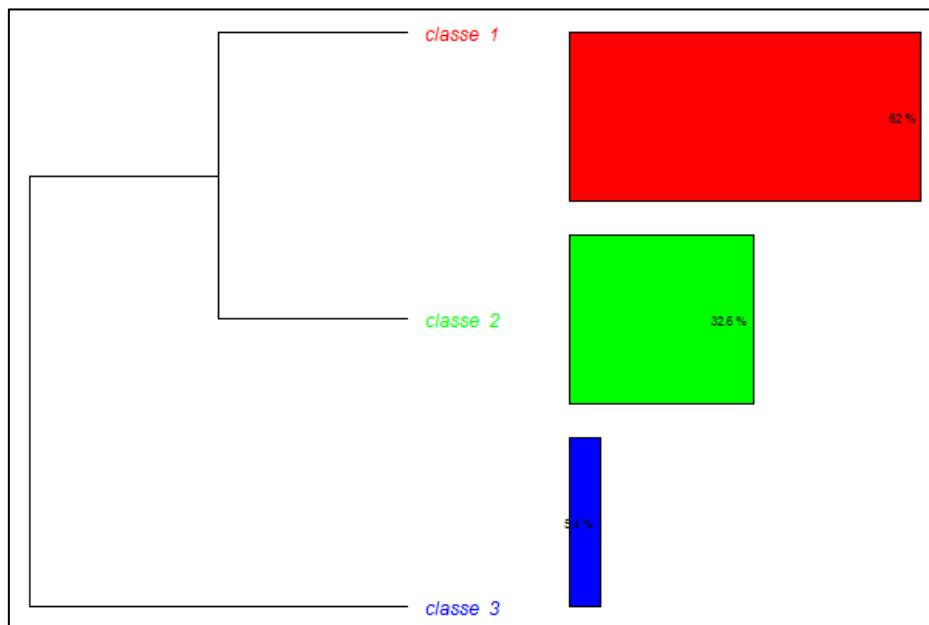


Figure 13 – Chi2 - Classification hiérarchique descendante des segments « cyber ». Corpus n°2

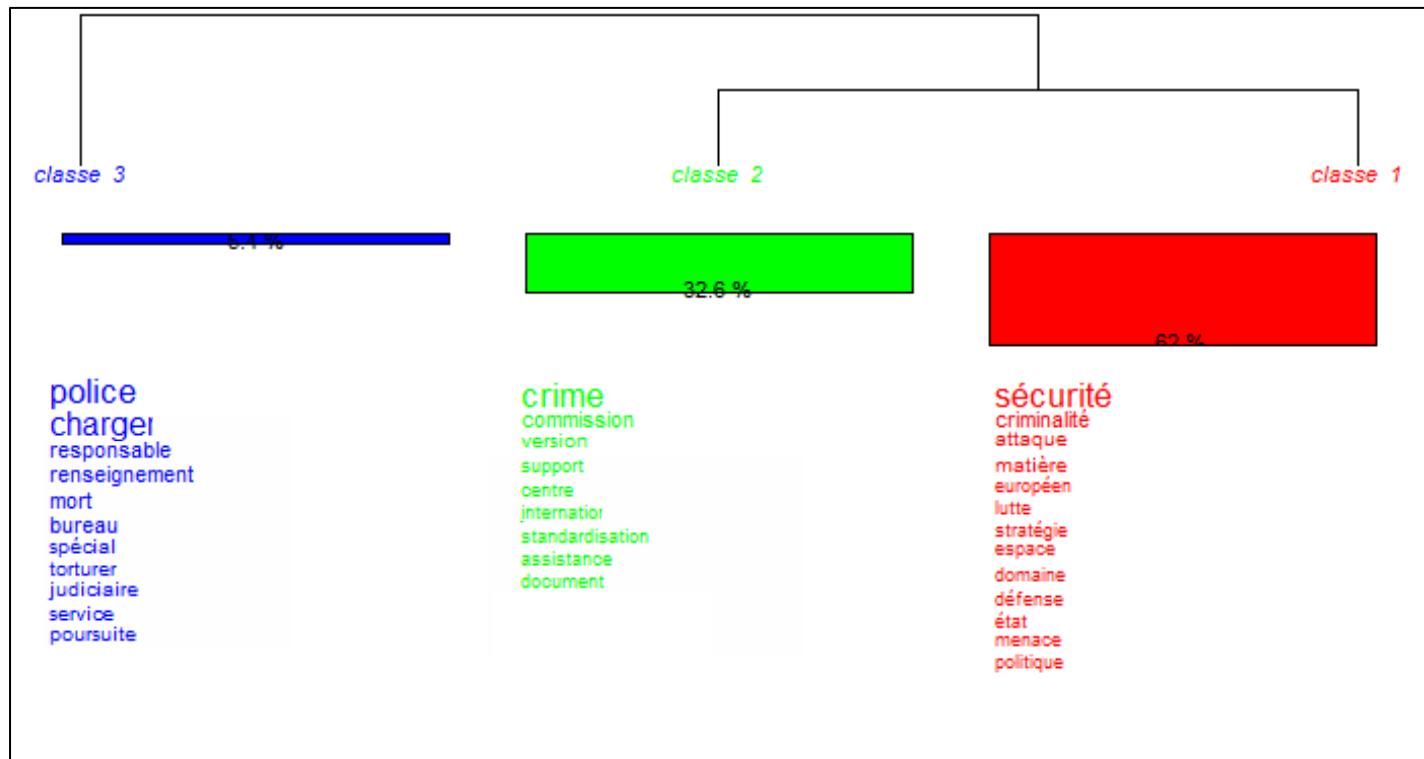


Figure 14 – Chi 2 - Formes les plus représentatives de chaque classe. Corpus n°2

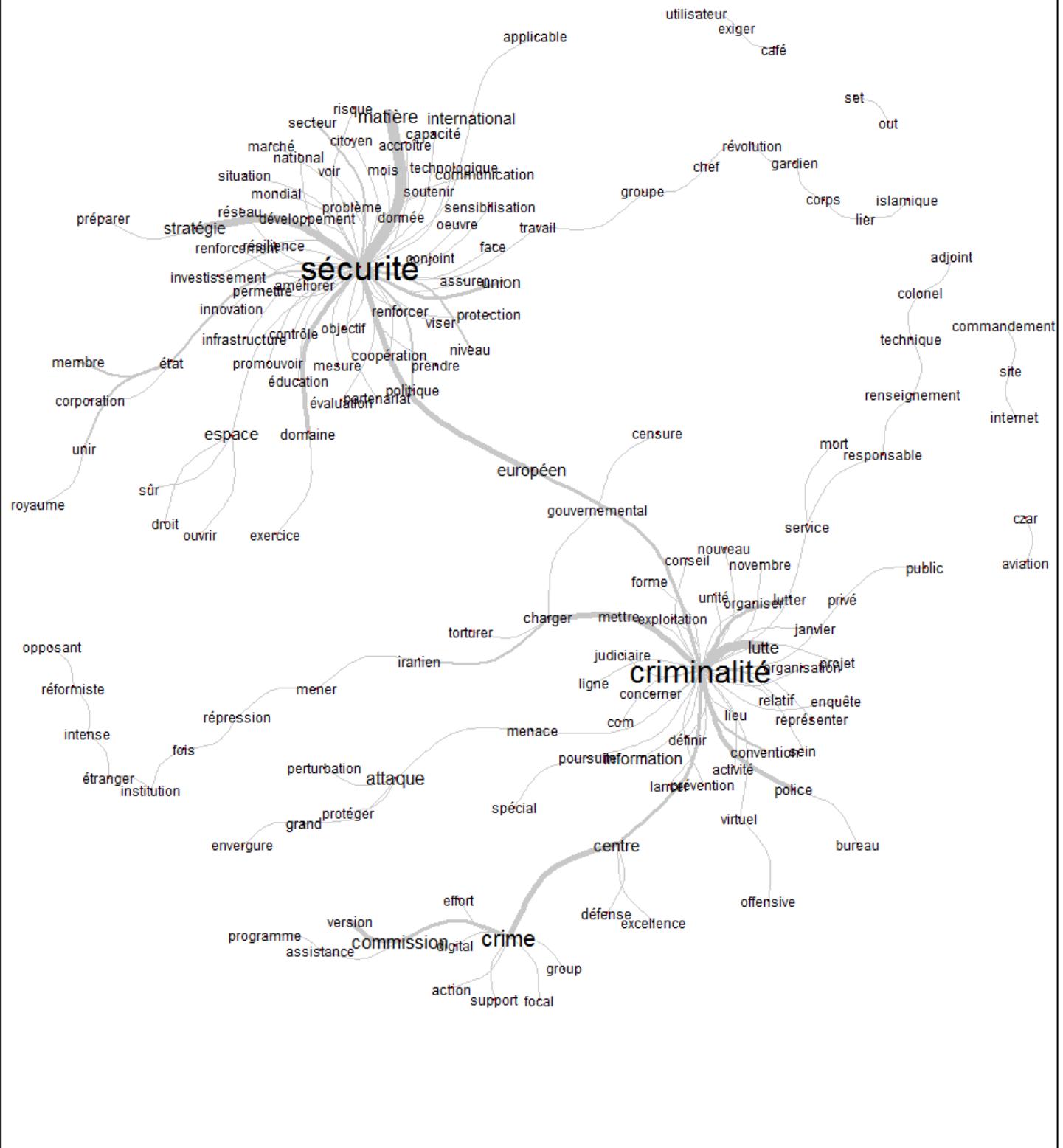


Figure 15 – Analyse de similitude en l'absence des termes « cyber ». Corpus n°2

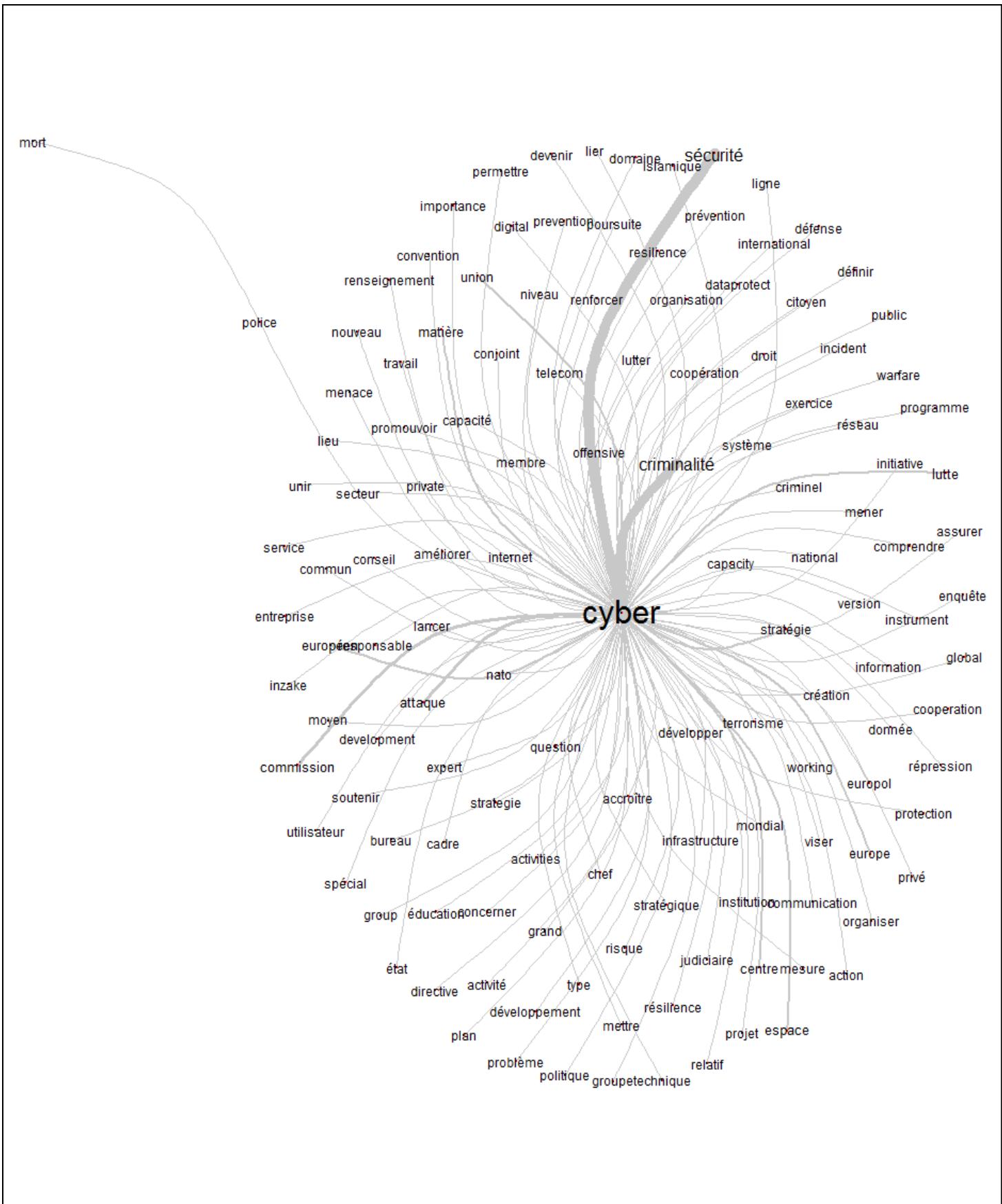


Figure 16 – Analyse de similitude à partir des termes « cyber ». Corpus n°2

2 – Résultats des approches thématiques : mondes lexicaux et analyse de similitude (Corpus 2).

Cette sous-section vise à nouveau deux types de résultats : ceux de la classification hiérarchique descendante sur le corpus 2 sont présentées en premières (**Figures 13 et 14**), suivies des analyses de similitudes sur le même corpus (**Figures 15 et 16**). La classification hiérarchique descendante a abouti sur ce corpus à 3 classes :

- La classe 1 (62% du corpus) qui concerne la sécurité de l'information, dont les substantifs les plus représentés sont : « sécurité », « criminalité », « attaque », « matière », ...
- La classe 2 (32,6% du corpus) qui touche aux aspects policiers et administratifs du cyberespace, dont les substantifs les plus représentés sont : « crime », « commission », « version », « support », ...
- La classe 3 (5,4% du corpus) qui relève essentiellement de la répression et de la surveillance, avec : « police », « charger », « renseignement », « responsable », ...

La différence n'est pas évidente entre les classes 2 et 3. Sinon que la classe 2 déterminerait une réponse fondée sur la coopération, tandis que la classe 3 correspondrait à une réponse active. Ces deux classes associées représentent 38% du corpus⁵⁹⁸.

Cette bipolarisation de sens autour du cyberespace dans le corpus 2 est également illustrée par les analyses de similitudes⁵⁹⁹. Lesquelles construisent deux regroupements de sens autour de la « criminalité » et la « sécurité ». Le poids de chacun des regroupements principaux vient occulter les regroupements secondaires. Il en ressort une certaine cohérence des segments ciblés dans le corpus, et donc une cohérence de sens au niveau européen dans l'emploi de terme dérivés du cyberespace. Le corpus « défense » n'est pas apparent dans le langage européen autour du cyberespace même si on peut identifier un certain nombre de substantifs qui peuvent lui être reliés. La présence d'un certain nombre de document spécifiquement consacrés à la

⁵⁹⁸ Il est possible de les associer notamment au regard de l'analyse de similitude (**Figure 15**) qui place les deux ensembles dans un même regroupement.

⁵⁹⁹ La matrice de similitude est calculée à partir de l'indice de cooccurrences des termes avec un seuil minimal fixé empiriquement à 10 pour la lisibilité des résultats. Ce seuil est plus important que précédemment du fait du nombre important de substantifs identifiés par le logiciel. La taille du texte et l'épaisseur des traits indiquent en relatif l'importance des occurrences du terme ainsi que la force des relations de cooccurrences qu'il entretient avec les autres éléments du corpus.

sécurité de l'information joue sans doute un rôle important dans cette tendance du corpus qui vient déconstruire l'idée reçue selon laquelle l'Europe ne se préoccupe pas de cybersécurité (cette préoccupation est aussi récente que celles des autres corpus).

C – Analyse documents de l'ONU de l'Organisation des Nations Unies en français entre 2001 et 2016.

Corpus n°3 - Cyber DOC ONU 2001-2016	
« Ensemble des publications du système de diffusion électronique des documents de l'ONU en français entre 2001 et 2016 contenant le mot cyberespace ou un terme dérivé. »	
Date de début : 1^{er} février 2001	
Date de fin : 31 octobre 2016	
Nombre de documents retenus : 218 sur 304 résultats	Nombre d'occurrences de termes « cyber » : 1158 <ul style="list-style-type: none">• 2001 à 2005 (inclus) : 32• 2006 à 2010 (inclus) : 174• 2011 à 2016 (inclus) : 952

Figure 17 – Descriptif du corpus d'étude « Cyber DOC ONU 2001-2016 ».

Contrairement aux corpus 1 et 2, ce troisième corpus (**Figure 17**) n'est pas le fruit d'une recherche sur un journal officiel particulier, mais sur le Système de diffusion électronique des documents (Sédoc) de l'Organisation des Nations Unies⁶⁰⁰. Lequel comprend à la fois des documents faisant l'objets de mesures de publicités mais aussi divers rapports, et également

⁶⁰⁰ Créé en 1993, le Sédoc contient les documents créés directement sous format électronique depuis 1993, par exemple les documents du Conseil de sécurité, de l'Assemblée générale, du Conseil économique et social et de leurs organes rattachés, les textes administratifs entre autres.... Sans être exhaustif, il renferme également la version numérisée de nombreux documents publiés de 1946 à 1993, notamment toutes les résolutions des organes principaux, tous les documents du Conseil de sécurité et les documents officiels de l'Assemblée générale. Les documents sont disponibles dans les six langues officielles de l'Organisation des Nations Unies et certains sont également disponibles en allemand. L'ONU autorise les utilisateurs à visiter le site et à télécharger ou copier des renseignements et des documents à des fins personnelles et non commerciales [...], <https://documents.un.org/>

divers éléments de travaux en cours. La période d'analyse est toujours la même. Ce troisième corpus a permis d'identifier 304 résultats, dont 218 ont pu être retenus dans le cadre de cette analyse. La raison est notamment que de nombreux documents récoltés ne font état que d'utilisation de noms propres ou de noms de lieu, exclus par nature de cette analyse⁶⁰¹. Les autres motifs d'exclusions sont identiques à ceux précédemment mobilisés. Comme pour l'Union Européenne, l'ONU diffuse souvent des prises de positions ou des rapports qui sont l'objets de différentes itérations et de commentaires⁶⁰². L'ensemble des documents y est plus diversifié que sur n'importe quel autre corpus. Cet état de fait est compensé par la valeur contraignante relativement faible de la très grande majorité des textes publiés (ce qui constitue également une spécificité de cet ensemble dans l'ensemble des discours institutionnels analysés). Ces spécificités ainsi la prise en compte de l'environnement complexe de l'ONU conduisent à la réaffirmation du principe selon lequel il faut regarder les données obtenues comme un produit d'échange d'idées entre les différentes composantes d'une organisation vaste et complexe plutôt que l'affirmation d'une conception unifiée propre à l'ensemble des acteurs au sein de l'ONU. A nouveau, l'intégration des documents dans le corpus a été effectuée en tenant compte de leur nature et de leur date de signature. L'ensemble documentaire a été nettoyé de sa mise en forme (tableaux, listes...) et redécoupé en segments.

Les opérations conduites sont sensiblement les mêmes que pour les corpus n°1 et 2 :

1. Le recensement de toutes les occurrences du terme cyberespace et des termes dérivés (**Figure 18**).
2. L'agrégation dans un sous-corpus de l'ensemble des segments de textes concernés par la première opération.
3. Une classification hiérarchique descendante (chi 2) (**Figures 19 et 20**).
4. Une analyse de similitude fondées sur les cooccurrences sans et avec la prise en compte de l'affixe « cyber » (**Figures 21 et 22**).

⁶⁰¹ Se retrouvent ainsi de nombreuses mentions d'un prestataire de service de l'ONU dont la dénomination comporte notamment « cyber » ainsi que tous les programmes des événements de l'ONU retransmis grâce à une « cyber salle de conférence ».

⁶⁰² Paradoxalement, le phénomène n'est pas aussi important dans ce troisième corpus (ONU) que dans le second (UE). Il n'y a aura donc pas le même phénomène de bipolarisation du discours.

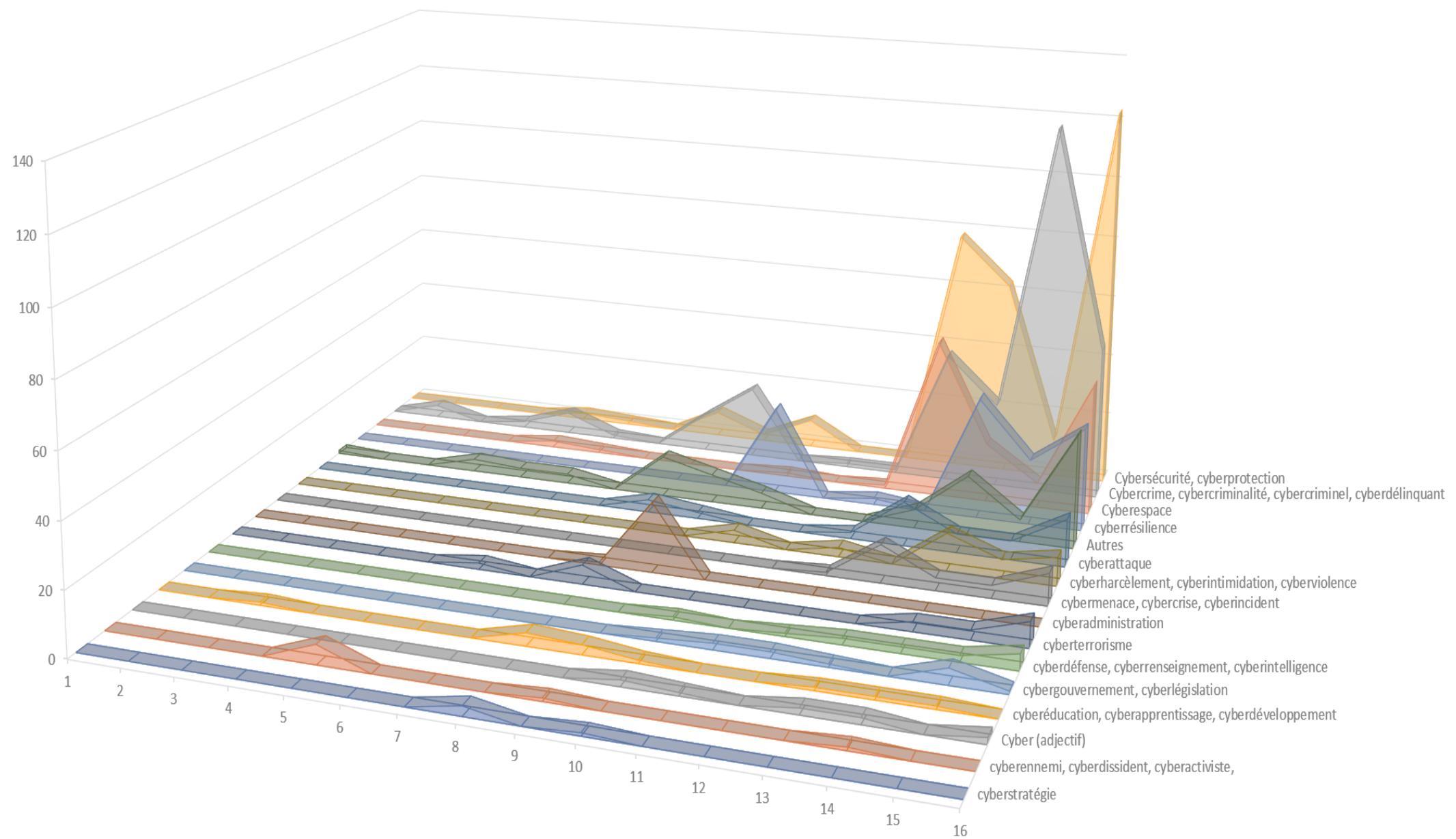


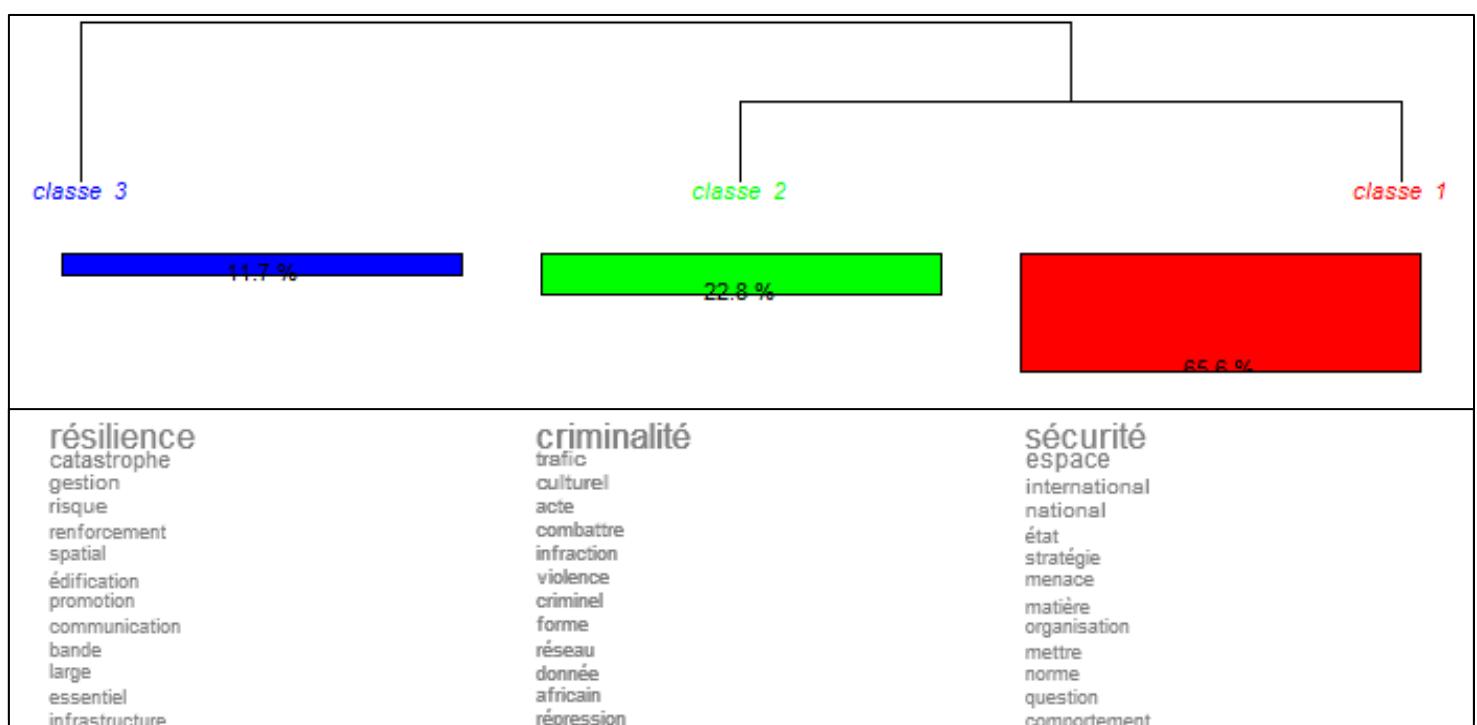
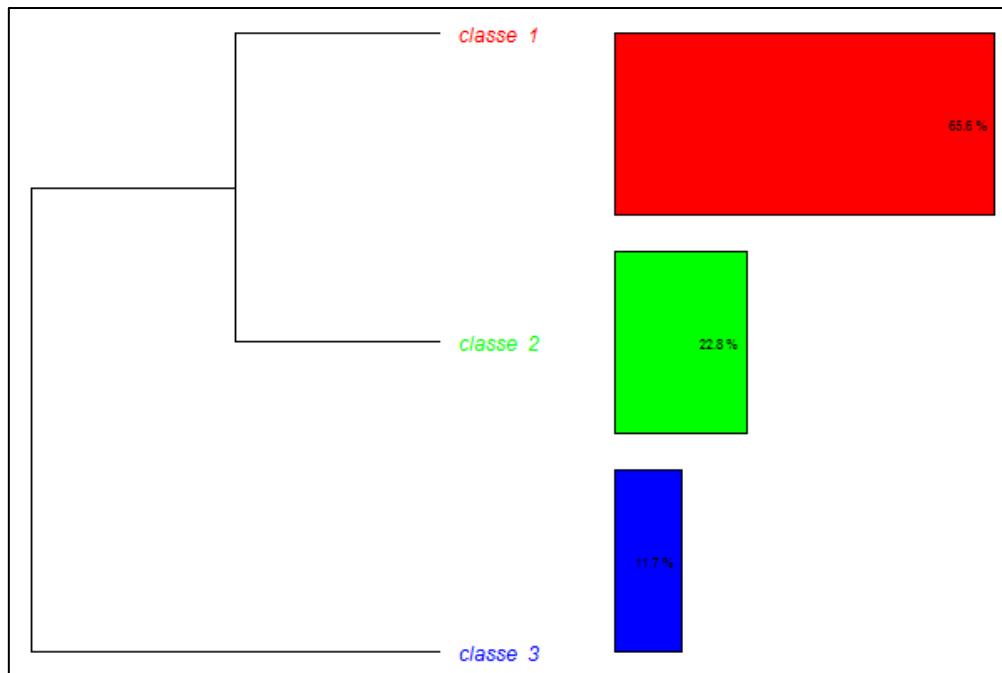
Figure 18 – Recensement des occurrences des termes « cyber ». Corpus n°3

1 – Analyse des résultats du recensement (Corpus 3).

Comme pour les corpus précédents les occurrences des termes « cyber » apparaissent de manière croissante dans le temps (**Figure 17**). Sur les 1158 occurrences identifiées, 82.21% (952) se produisent entre 2011 et 2016. Si la tendance est la même sur le plan du nombre, il y a quelques variations dans les termes qui apparaissent le plus (**Figure 18**).

En effet, si on retrouve les désormais classiques groupements de termes autour de la « cybersécurité » (25.73% des occurrences) et du « cybercrime » (24.96%), ce corpus met en valeur d'autres idées de manière relativement inédite par rapport aux autres discours institutionnels. « cyberespace » (10.79%) retrouve ici son utilisation majoritaire dans le cadre des libertés publiques mais plus généralement dans tous les enjeux tels que le droit d'accès, le comportement ou encore l'éthique. Les termes du groupe « cyberrésilience » (10.62%) sont d'un usage plus commun que dans les autres corpus. Le groupe « autre » (9.15%) est probablement l'un des plus présents parmi les discours institutionnels⁶⁰³. Ainsi, en dépit d'un lexique moins précis et des spécificités qui ont été mentionnées, ce troisième corpus vient s'inscrire dans la dynamique des autres discours institutionnels en mentionnant des utilisations majoritaires de termes dérivés du cyberespace identiques. Toutefois, l'écart entre les premiers résultats en nombre d'occurrences et les suivants est bien plus réduit que pour les corpus précédents ce qui laisse présager à ce stage de l'analyse une configuration plus large des cooccurrences au niveau des thèmes abordés. L'introduction des dérivés du cyberespace au niveau de l'ONU semble pleinement consacrée à partir de 2009 et connaît un vif essor à partir de 2014. Dates à partir desquelles le corpus adopte ses tendances actuelles. Ce qui signifie que les termes ont été plus rapidement en usage au niveau de l'ONU qu'au niveau de l'Union européenne. Quelques itérations antérieures à ces dates viennent confirmer ce dernier état de fait⁶⁰⁴. Les occurrences antérieures à 2009, au nombre de 91 tous termes confondus représentent 7.86% du total des occurrences. Sur cette période, c'était le cybercrime qui tenait la première place et représentait alors 28.6% du total entre 2001 et 2009.

⁶⁰³ C'est également l'un des plus riches au niveau de la variété des itérations et des domaines concernés. Il comprend notamment cyberagriculture, cybersanté, cyberenvironnement, cybernétique, cybercafé, cyberjournaliste, cyber île, cybervmédia, cyber caravane, cyber paiement, cyberpolice, cyberpatrouille, cybervolontaire, cyber bien-être, cybercommunautés, cyberafrique, cyberworld [...]



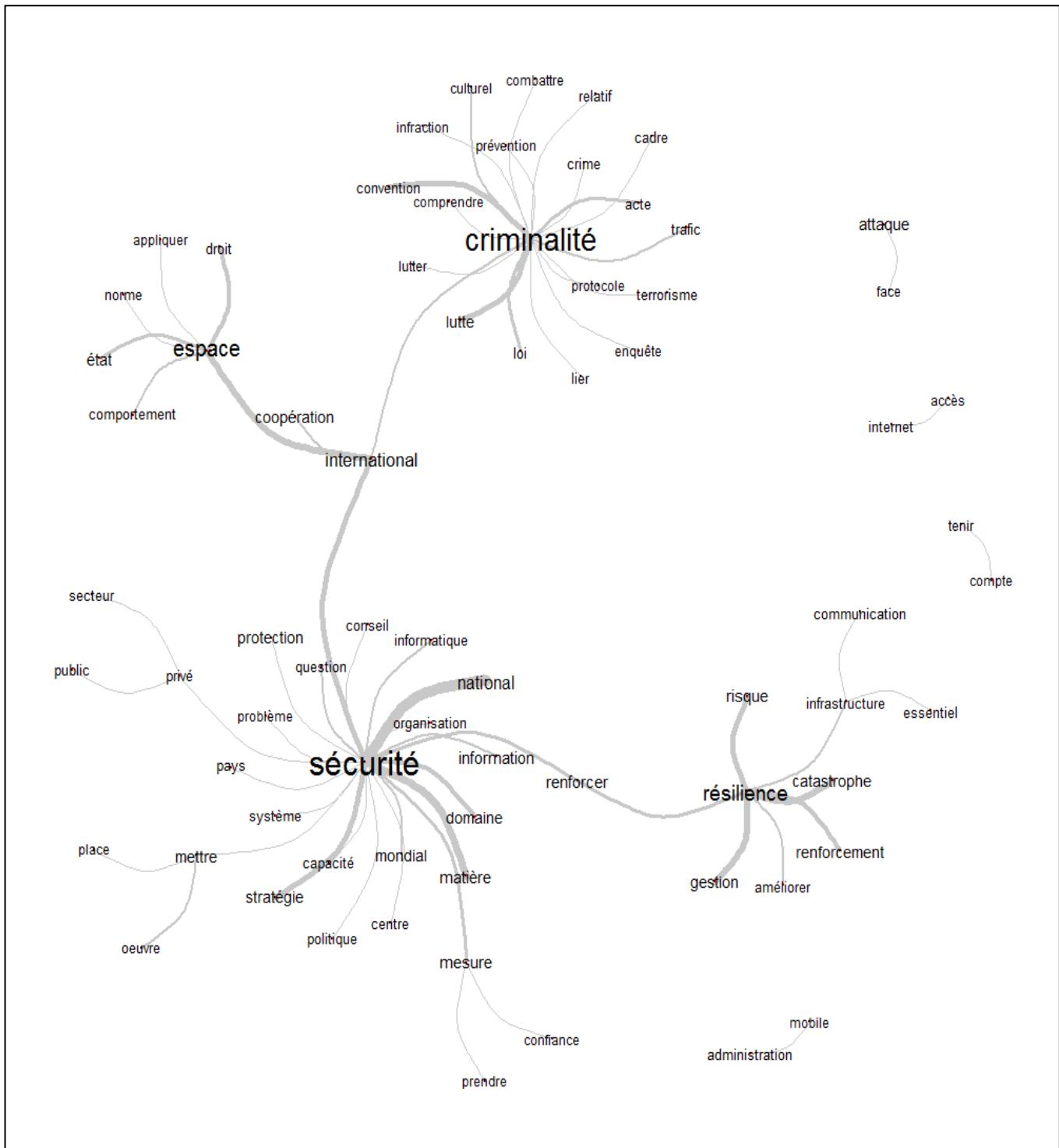


Figure 21 – Analyse de similitude en l'absence des termes « cyber ». Corpus n°3

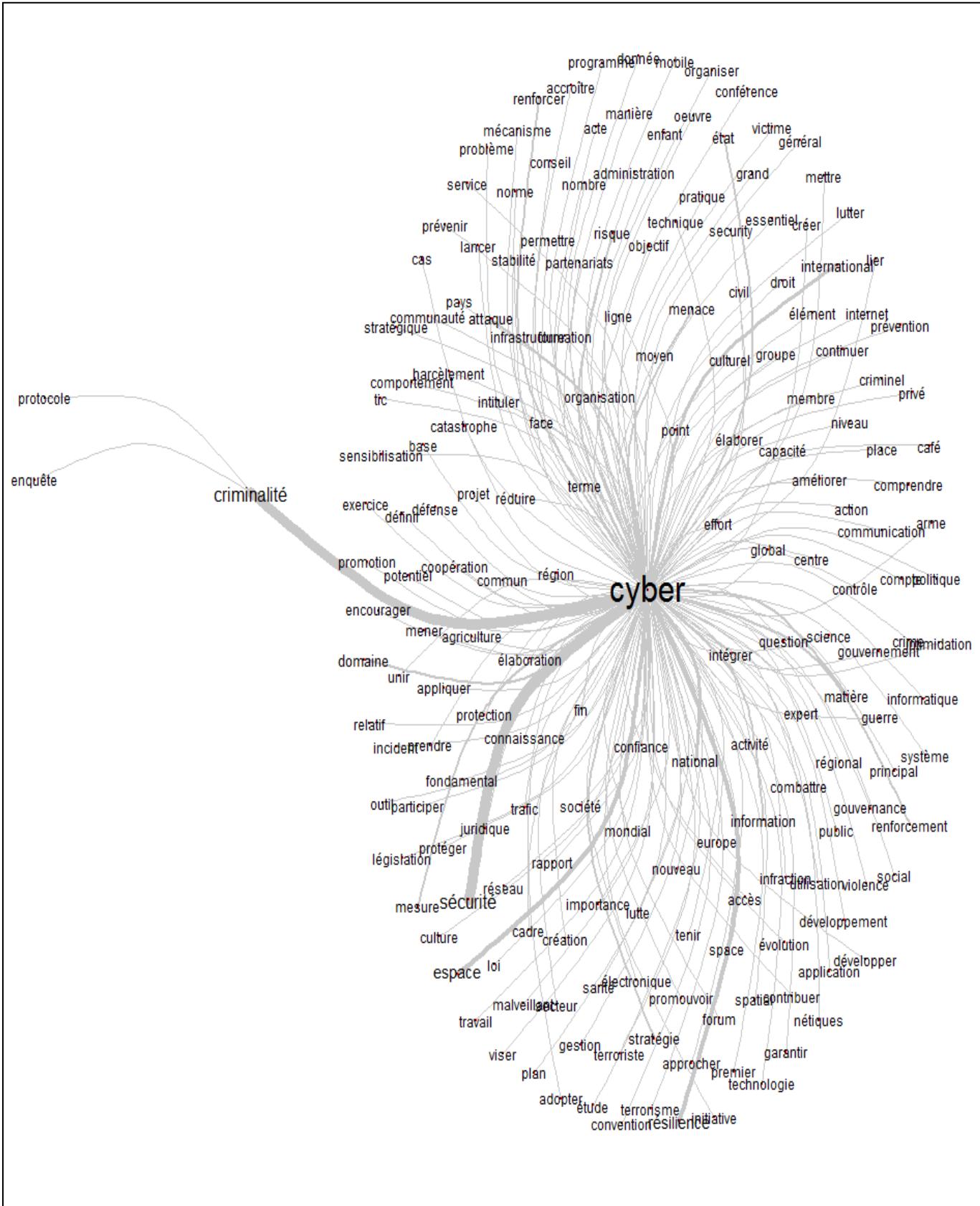


Figure 22 – Analyse de similitude à partir des termes « cyber ». Corpus n°3

2 – Résultats des approches thématiques : mondes lexicaux et analyse de similitude (Corpus 3).

Entre la classification hiérarchique descendante (**Figures 19 et 20**) et les analyses de similitudes (**Figures 21 et 22**), le corpus 3 présente des spécificités intéressantes par rapport aux deux premiers. Les classes identifiées sont les suivantes :

- La classe 1 (65,6% du corpus) qui concerne l'enjeu stratégique de l'information, dont les substantifs les plus représentés sont : « sécurité », « espace », « international », « national », « État » (État), ...
- La classe 2 (22,8% du corpus) qui touche aux aspects policiers du cyberespace, dont les substantifs les plus représentés sont : « criminalité », « trafic », « culturel », « acte », « combattre » ... Cette dernière est intégrée avec la classe 1 dans le même sous ensemble hiérarchique.
- La classe 3 (11,7% du corpus) qui relève essentiellement de l'appréhension du risque, avec : « résilience », « catastrophe », « gestion », « risque », ... La classe 3 figure à part dans la hiérarchie des classes.

Il y a une forte représentation de la classe 1 au sein de ce corpus. Laquelle couple à une forte spatialisation de l'information avec une vision sécuritaire de celle-ci. Néanmoins les deux autres classes sont également essentielles en ce qu'elles concernent majoritairement d'une part la criminalité et la gestion du risque autour de l'information. Si la criminalité demeure une thématique forte quel que soit le corpus, la résilience semble ici suivre un chemin plus spécifique : plus le lieu d'échange est international, plus la résilience est un thème fort des échanges⁶⁰⁵. Néanmoins, la résilience fait figure d'un thème un peu à part moins au centre que ne peuvent y être la « sécurité » ou la « criminalité » qui forment le cœur des segments identifiés.

Si elle possède les mêmes tendances, l'analyse de similitude dégage quatre grappes principales : « sécurité », « criminalité », « espace », « résilience », ainsi que quelques éléments

⁶⁰⁵ Une comparaison avec la production anglophone de l'OTAN, du *World Economic Forum*, va également dans ce sens. Il semble que ce soit également le cas des entretiens réalisés qui en fonction du niveau institutionnel de la personne ont tendance à laisser plus de place à la résilience. Même si au niveau national, la résilience demeure un thème émergent.

extérieurs. La convergence principale au niveau des grappes s'établit autour du substantif « international » (relié de très près à la « coopération »). Seule la grappe « résilience » est mise à part et construit ses liens majeurs avec la grappe « sécurité » notamment par le lien « sécurité – renforcer – résilience ». Les enjeux du corpus 3 apparaissent globalement plus variés que ceux des corpus 1 et 2, cela se traduit par une forte prise en compte des enjeux sociaux et des enjeux des libertés individuelles dans des proportions plus importantes. A l'image du corpus 2, « criminalité » et « sécurité » sont les grappes les plus importantes et elles interagissent avec des substantifs souvent comparables pour les plus représentatifs d'entre eux.

D – Synthèse des résultats 2001-2016 sur les corpus 1, 2 et 3 :

Présentés principalement sous formes de tables et de graphes, ces résultats intègrent d'une part, la synthèse des différents recensements des occurrences (1, **Figure 23 à 26**), d'autre part la synthèse des substantifs les plus représentatifs pour chaque classe de chaque corpus dans les classifications hiérarchique descendante (2,**figure 27**), et enfin une projection des principaux substantifs identifiés dans les analyses de similitude (3. **figure 28**).

1 – Recensement d'occurrences - variations des termes « cyber » :

Corpus 1			Corpus 2			Corpus 3		
Groupes	Résultats	%	Groupes	Résultats	%	Groupes	Résultats	%
Cybercrime, cybercriminalité, cybercriminel, cyberdélinquant	35	22,73%	Cybersécurité, cyberprotection	1251	45,15%	Cybersécurité, cyberprotection	298	25,73%
cyberdéfense	27	17,53%	Cybercrime, cybercriminalité, cybercriminel, cyberdélinquant	797	28,76%	Cybercrime, cybercriminalité, cybercriminel, cyberdélinquant	289	24,96%
Cybersécurité, cyberprotection	17	11,04%	cyberattaque	220	7,94%	Cyberespace	125	10,79%
cyberdiplomatie	17	11,04%	cyberdéfense	101	3,64%	cyberrésilience	123	10,62%
Cyber (adjectif)	12	7,79%	cybermenace, cybercrise, cyberincident	100	3,61%	cyberattaque	106	9,15%
cyberdissident, cyberennemi	10	6,49%	Cyberespace	85	3,07%	cyberharcèlement, cyberintimidation, cyberviolence	49	4,23%
Autres	36	23,38%	Autres	217	7,83%	Autres	168	14,51%
Total	154		Total	2771		Total	1158	

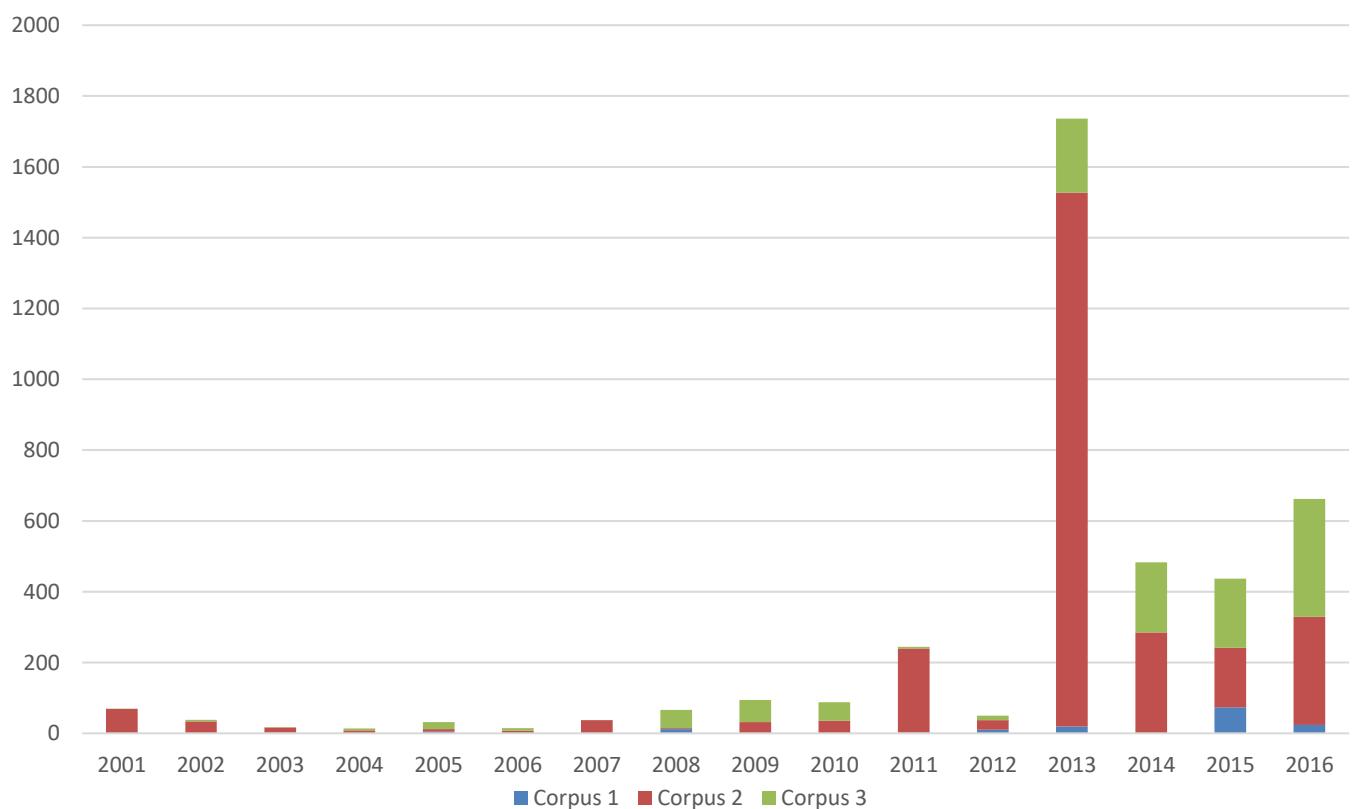
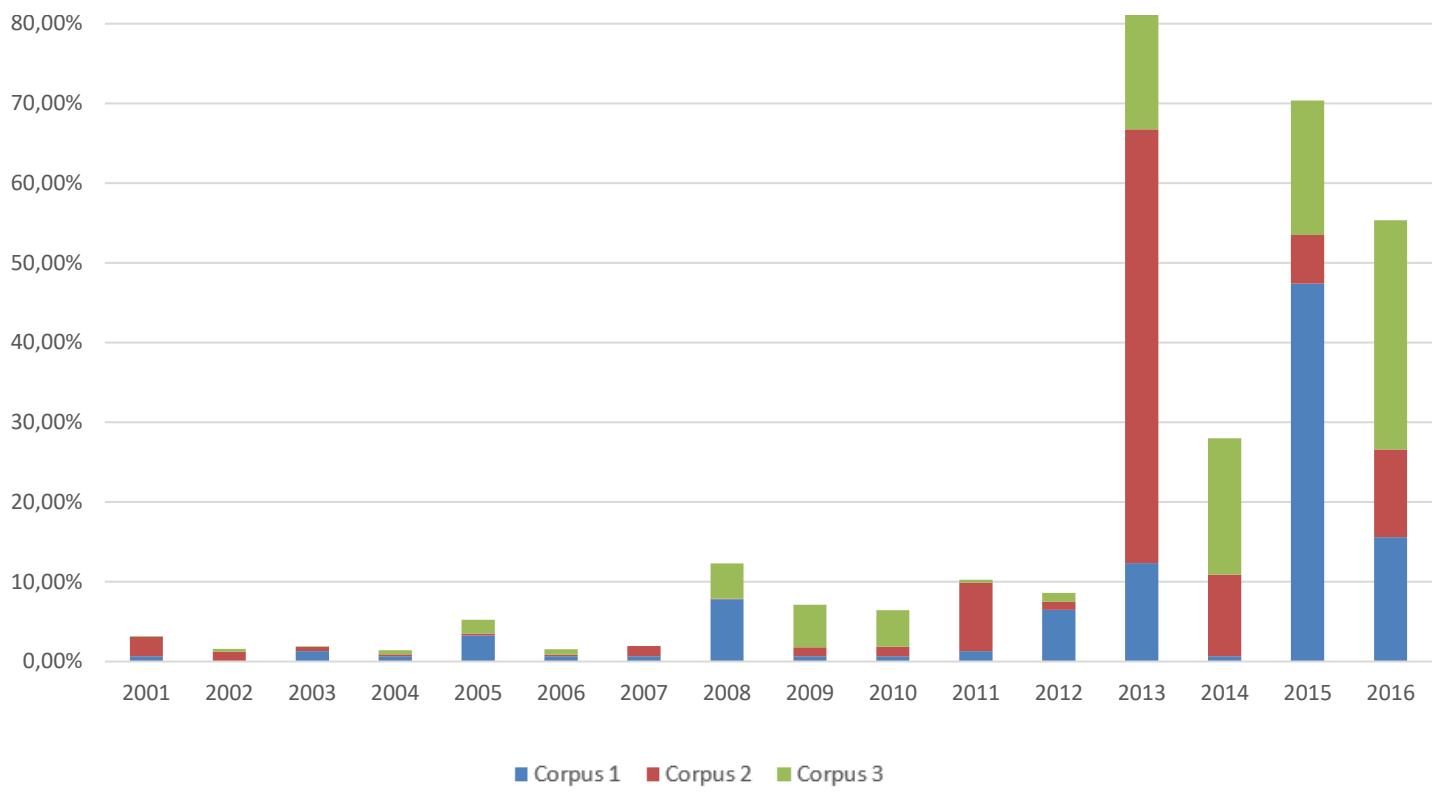
Figure 23 – Calculs des occurrences – groupes de substantifs principaux par corpus (en nombres et pourcentages)

Année	Corpus 1	%	Corpus 2	%	Corpus 3	%
2001	1	0,65%	68	2,45%	1	0,09%
2002	0	0,00%	34	1,23%	4	0,35%
2003	2	1,30%	14	0,51%	1	0,09%
2004	1	0,65%	7	0,25%	6	0,52%
2005	5	3,25%	7	0,25%	20	1,73%
2006	1	0,65%	6	0,22%	8	0,69%
2007	1	0,65%	36	1,30%	0	0,00%
2008	12	7,79%	3	0,11%	51	4,40%
2009	1	0,65%	31	1,12%	62	5,35%
2010	1	0,65%	34	1,23%	53	4,58%
2011	2	1,30%	238	8,59%	4	0,35%
2012	10	6,49%	27	0,97%	13	1,12%
2013	19	12,34%	1508	54,42%	209	18,05%
2014	1	0,65%	284	10,25%	198	17,10%
2015	73	47,40%	169	6,10%	195	16,84%
2016	24	15,58%	305	11,01%	333	28,76%
Totaux	154	100%	2771	100%	1158	100%

Légende

- Valeurs les plus fortes par corpus
- Valeurs les plus faibles
- ➡ Années avec le plus de résultats en pourcentage (voir figure 25)

Figure 24 – Calculs des occurrences – Résultats totaux par année et par corpus (en nombre et en pourcentages)



Figures 25 et 26 – Projections des résultats de calcul des occurrences en pourcentages des résultats exprimés par corpus et en résultats exprimés par corpus

2 – Classifications hiérarchiques descendantes :

[Pour chaque corpus, chaque classe (en %) substantifs les plus représentatifs (chi2)]

Corpus 1							
Classe 1	39,02%	Classe 2	21,95%	Classe 3	14,63%	Classe 4	24,39%
espace	13,37	défense	106,02	dissident	49,91	sécurité	57,02
criminalité	8,16	intégrer	18,53	Ligne	43,3	attaque	23,01
territoire	4,8	opérationnel	14,7	diplomatie	30,4	particulier	12,82
police	4,8	organisation	13,87	international	24,12	terrorisme	12,82
general	4,8	posture/force	10,93	Politique	6,66	entreprise	12,82

Corpus 2					
Classe 1	61,98%	Classe 2	32,58%	Classe 3	5,44%
sécurité	410,67	crime	305,91	Police	707,47
criminalité	116,73	commission	107,54	Charger	626,2
attaque	86,41	version	78,06	responsable	385,68
matière	66,13	support	37,53	renseignement	196,75
européen	56,72	centre	35,78	Mort	191,95

Corpus 3					
Classe 1	61,98%	Classe 2	32,58%	Classe 3	5,44%
sécurité	137,07	criminalité	269,77	Résilience	348,43
espace	60,7	trafic	55,26	catastrophe	266,32
international	34,07	culturel	48,23	Gestion	185,01
national	25,7	acte	36,28	Risque	119,26
état	18,85	combattre	29,41	renforcement	67,35

Figure 27 - Classifications hiérarchiques descendantes, substantifs les plus représentatifs de chaque classe

3 – Analyses de similitudes – principaux substantifs :

Cette synthèse ne tient compte que des principaux à l'exclusion des « îlots » et des résultats dont l'indice de cooccurrence était trop éloigné des indices les plus importants.

Cyber <i>Discours institutionnels</i>		
Corpus 1 <i>France</i>	Corpus 2 <i>UE</i>	Corpus 3 <i>ONU</i>
<p>1. Criminalité → Lutte → Travail → Convention → Ressource</p> <p>2. Défense → Organisation → Armée → Intégrer → Opérationnel</p> <p>3. Sécurité → Entreprise → Système → Centre / Maritime</p>	<p>1. Sécurité → Stratégie → Matière → Européen</p> <p>2. Criminalité → Lutte/lutter → Convention → Européen → Matière/sécurité</p>	<p>1. Sécurité → Matière / Domaine → International → Stratégie / Mesure → National</p> <p>2. Criminalité → Lutte → Convention → Acte / trafic / loi</p> <p>3. Espace → Droit → État → Comportement</p> <p>4. Résilience → Risque → Gestion → Catastrophe → Renforcement</p>

Figure 28 – Synthèse des analyses de similitudes sur les corpus 1, 2 et 3

Section 2 – La thématique « cyber » dans la presse écrite francophone :

L’analyse de la presse écrite en complément de l’analyse de la production institutionnelle présente plusieurs intérêts. Si le langage journaliste utilise comme la production institutionnelle un registre de langage soutenu, ses impératifs d’économie et d’accessibilité conditionnent certains traits particuliers qui peuvent être intéressants. Premièrement, le langage journalistique subit l’influence d’autres langages (droit, médecine, technique, économie) dont il doit rendre compte des évolutions.

Dans un second temps, le langage journaliste adopte un but : la recherche d’une audience. Là où par essence le langage institutionnel n’a pas besoin de séduire un public. L’économie d’un journal suppose de pouvoir attirer et retenir le lecteur. Le langage journaliste produit ainsi un discours se voulant proche des préoccupations individuelles du public, avec une portée générale, dans un système de sens conforme aux représentations sociales dudit public. Cet impératif diminue de fait la dépendance du langage journalistique à la spécialisation des définitions techniques, quitte à s’aliéner les spécialistes de ces mêmes définitions. En tant que tel, ce type de publications peut être compris comme un *medium* entre un discours institutionnel et un discours plus général. Il est donc possible d’interroger la spécificité de la représentation institutionnelle du langage cyber par rapport à une représentation commune inter-individuelle portée par les médias.

Là où la première analyse permettait de partir de l’État jusqu’aux « plus hautes » sphères supra-étatique, cette seconde approche permet de descendre à un niveau infra-étatique. Le degré spécialisé de certaines publications permettrait même avec plus de temps, d’avoir une approche par secteur. Néanmoins dans le cadre de cette recherche, nous nous concentrerons sur la délimitation d’un cadre général.

Cette recherche concernera plus spécifiquement deux corpus de données issus de deux agrégateurs de presse : factiva et google news.

A – Résultats à partir du moteur de recherche Factiva.

Corpus n°4 - Cyber Factiva FR 2001-2016

« Ensemble des publications francophones de presse généraliste et spécialisée entre 2001 et 2016 contenant le mot cyberespace ou un terme dérivé disponibles sur la plateforme Factiva. »

Date de début : 1^{er} février 2001

Date de fin : 31 octobre 2016

Nombre de documents retenus : 27957
sur 45221 résultats

Nombre de médias identifiés : 99

[Estimation totale du nombre d'articles publiés sur cette période 47 millions comptabilisés sur ces moteurs de recherche, tous sujets confondus]

Nombre d'occurrences de termes « cyber » : 36494

- 2001 à 2005 (inclus) : 4540
- 2006 à 2010 (inclus) : 9282
- 2011 à 2016 (inclus) : 22672

Figure 29 – Descriptif du corpus d'étude « Cyber Factiva FR 2001-2016 ».

Factiva est un agrégateur de presse de la société Dow Jones & Company auquel l'Université de Rennes 1 était abonné jusqu'en avril 2013. Il a été remplacé par son concurrent Europresse. Son nombre de sources francophones est d'environ 660 titres de presse. Les effets observés sur la structuration du corpus tiennent aux défauts précédemment constatés sur les autres corpus : d'une part, l'utilisation du préfixe « cyber » dans de nombreux noms propres ; d'autre part, de nombreuses copies d'articles. Alors que l'union européenne produisait de nombreuses versions consolidées des mêmes textes ici les mêmes articles sont souvent reproduits par les mêmes journaux. Encore une fois, les opérations conduites sont les mêmes que pour les autres corpus : Le recensement de toutes les occurrences du terme cyberespace et des termes dérivés (**Figure 30**), une classification hiérarchique descendante (chi 2) (**Figures 31 et 32**) et une analyse de similitude fondées sur les cooccurrences sans et avec la prise en compte de l'affixe « cyber » (**Figures 33 et 34**).

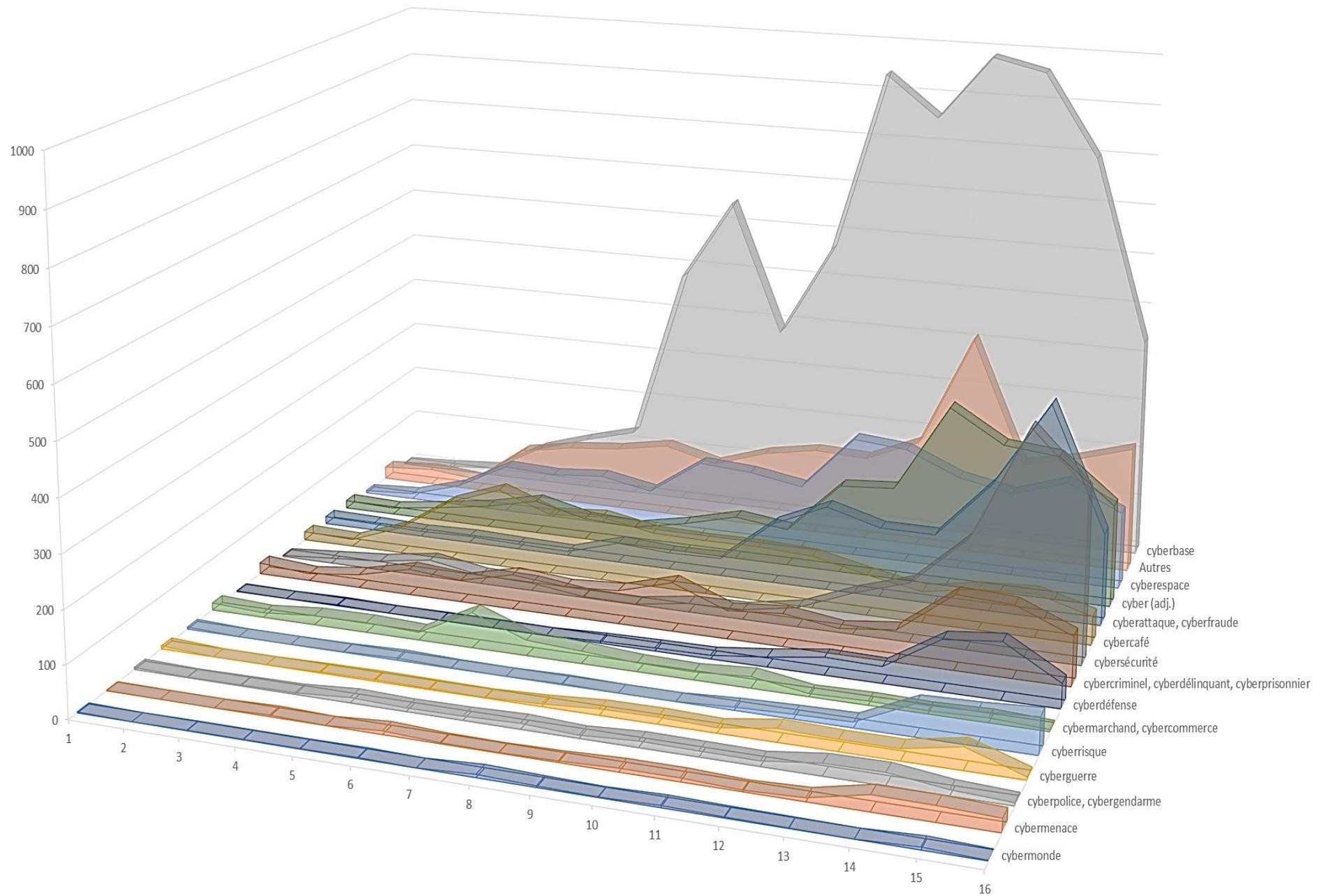


Figure 30 – Recensement des occurrences des termes « cyber ». Corpus n°4

1 – Analyse des résultats du recensement (Corpus 4).

Le total des occurrences connaît ici une progression similaire à celle des autres corpus (**Figure 29**). Le premier effet visible des occurrences de ce corpus est la domination de l'expression « cyberbase » qui incarne 20,26% des résultats entre 2001 et 2016 (7393 occurrences). Une cyberbase est un espace public numérique labellisé par la caisse des dépôts et consignation qui était délivré entre 1999 et 2014 à des lieux dédiés à l'apprentissage de l'informatique et d'Internet. Avec la forte occurrence de ce label et d'autres termes tels « cybercafé » se présente l'idée de l'impact de la presse locale sur la structuration du corpus. L'autre thématique forte dans les occurrences recoupe le lexique sécuritaire que l'on trouvait dans le discours institutionnel. Toutefois, même additionnés, ces groupes d'occurrences ne représentent que 13,77% du total (5025 occurrences).

Schématiquement, on pourrait définir la représentation du cyberspace comme quelque chose auquel il y a une nécessité d'accès et dont on peut subir diverses atteintes. Toutefois la thématique de l'accès semble prépondérante. Des thématiques marginales telles le commerce en ligne (« cybermarchand, cybercommerce »).

Entre les groupes d'occurrences liés à la sécurité ou à l'accès Internet, il est important de souligner les fortes occurrences du « cyberspace » en tant que tel, du nouvel adjetif « cyber » à partir de 2007, ainsi que du groupe des termes divers qui ne sauraient constituer une thématique du fait de leur diversités (deuxième groupe, avec 2496 occurrences). Cette force présence du cyberspace et de divers termes sont des traits communs avec l'ONU. Néanmoins, le corpus n°4 est plus riche dans ses exemples voire plus fantaisiste (on y retrouve le fameux « cyberfrigo », la « cyberabeille » et d'autres termes qui étaient absents du corpus n°3).

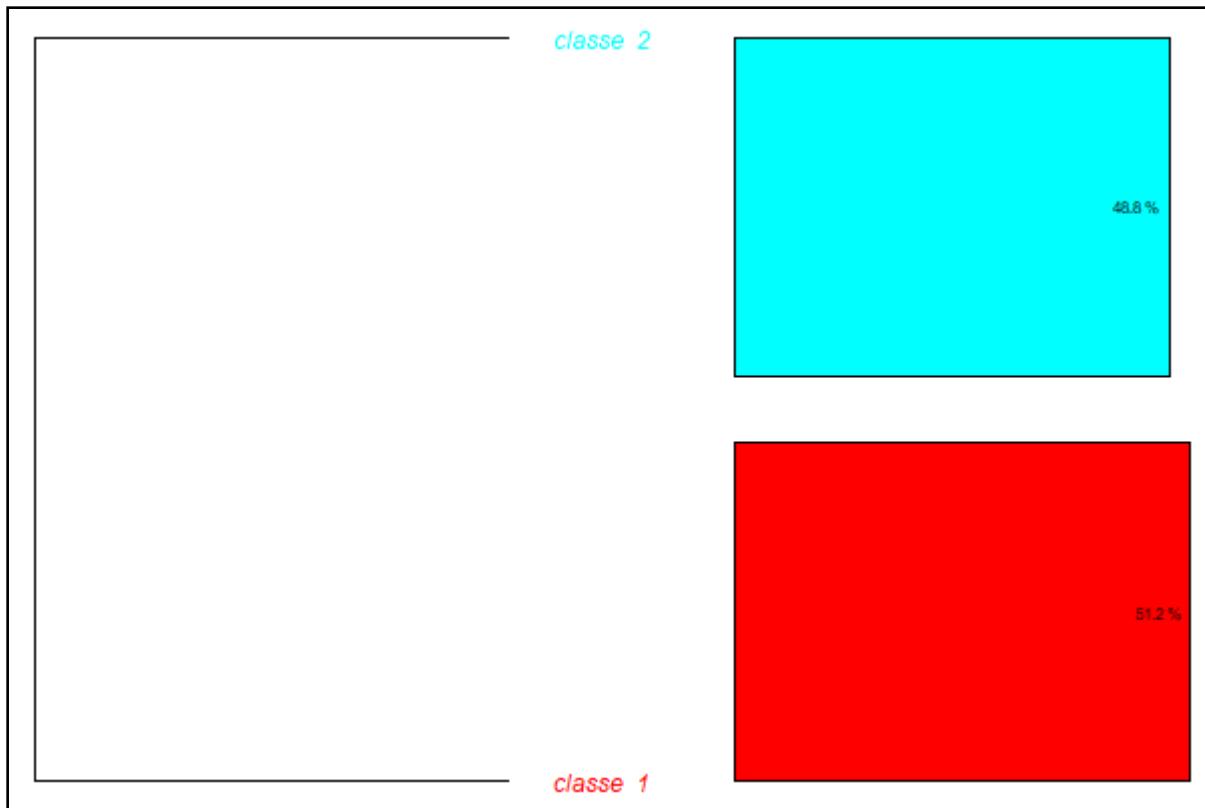


Figure 31 – Chi2 - Classification hiérarchique descendante des segments « cyber ». Corpus n°4

Classe 1 – 51,2 %		Classe 2 – 48,8 %	
Base	7052.72	Attaque	1636.66
Espace	1982.25	Sécurité	1276.51
Centre	1179.49	Harcèlement	721.04
Bibliothèque	988.2	Criminalité	609.86
Atelier	811.18	Défense	480.97
Café	469.18	Risque	429.58
Emploi	428.91	Menace	286.68

Figure 32 – Chi2 - Formes les plus représentatives de chaque classe (en chi2). Corpus n°4

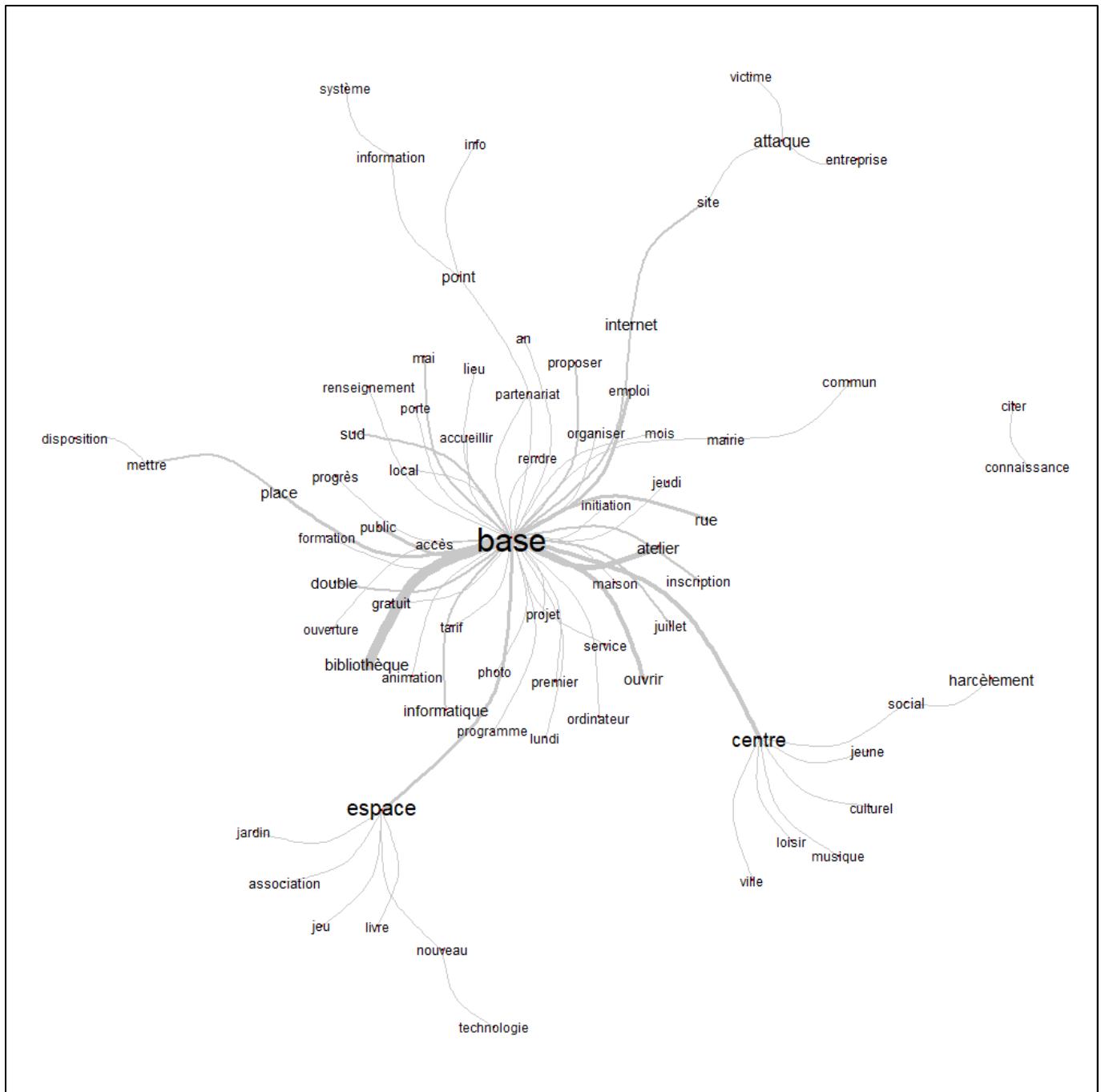


Figure 33 – Analyse de similitude en l'absence des termes « cyber ». Corpus n°4

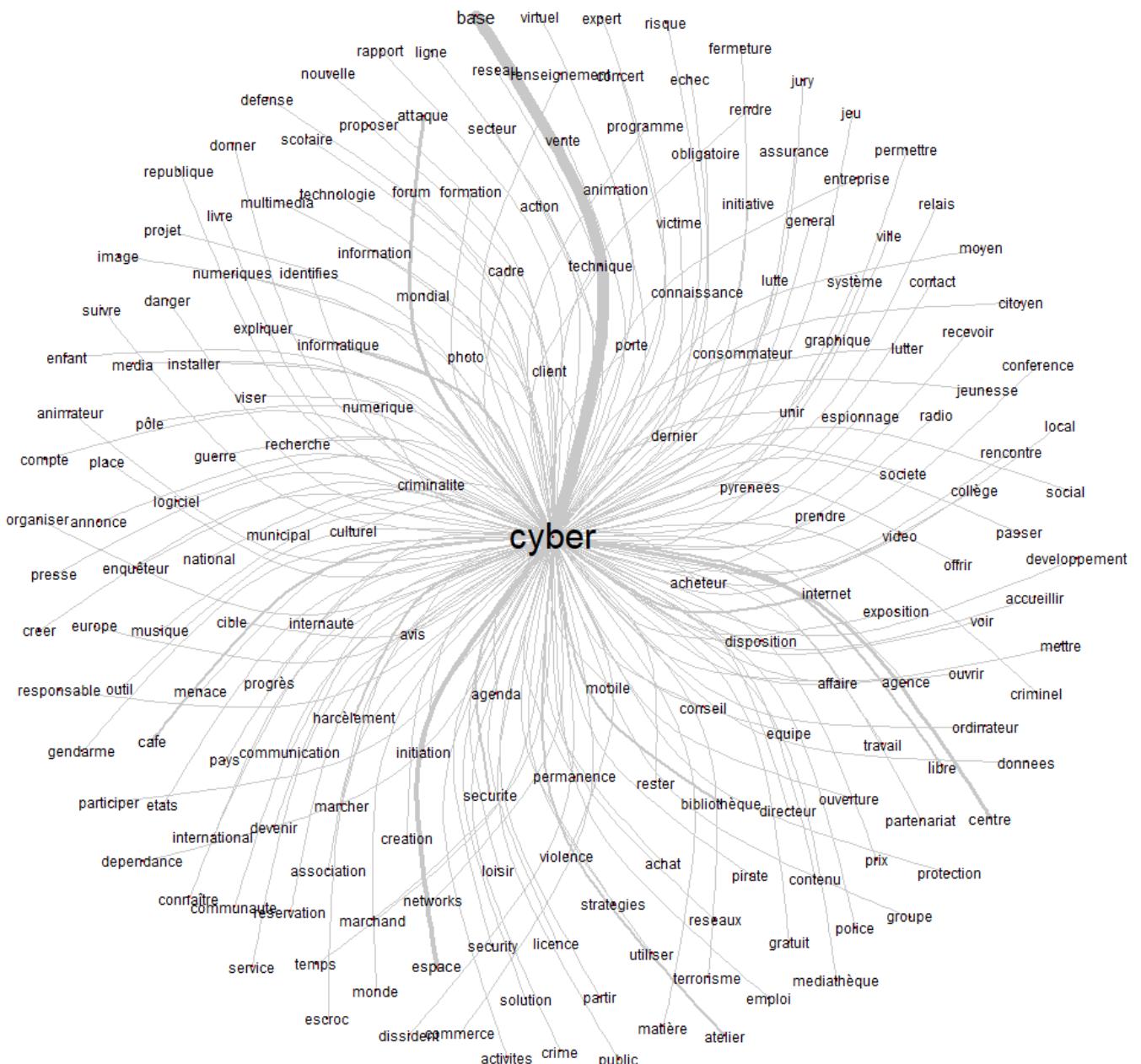


Figure 34 – Analyse de similitude à partir des termes « cyber ». Corpus n°4

2 – Résultats des approches thématiques : mondes lexicaux et analyse de similitude (Corpus 4).

La classification hiérarchique descendante (**Figures 31 et 32**) et les analyses de similitudes (**Figures 33 et 34**), sont particulièrement intéressantes concernant ce corpus car elles illustrent une construction du thème très polarisée. Les classes identifiées sont :

- La classe 1 (51,2% du corpus) qui concerne l'accès à l'information de manière générale, dont les substantifs les plus représentés sont : « base », « espace », « centre », « bibliothèque », « atelier », « café », « emploi ».
- La classe 2 (48,8 % du corpus) qui est concentrée sur la sécurité de l'information. « attaque », « sécurité », « harcèlement », « criminalité », « défense », « risque », « menace ».

Il n'y a aucune hiérarchie établie par le logiciel entre ces deux classes.

Il s'agit du premier corpus où le substantif « criminalité » ne tient pas l'une des premières places dans le discours sur la sécurité de l'information. Elle cède la place au substantif « attaque ». Si la « sécurité » est deuxième, le « harcèlement » vient en troisième position. La thématique de la sécurité de l'information semble viser les comportements dont les personnes privées sont victimes. De son côté la thématique de l'accès de l'information forme la thématique principale et se concentre principalement sur les lieux qui la permettre. Cette spatialisation touche également les autres substantifs de la classe « espace » et « emploi ».

L'analyse de similitude révèle une thématique centrale : l'accès à l'information concentrée autour substantif « base ». Si la thématique de la sécurité est bel et bien présente, elle existe de façon périphérique à cette première thématique. En effet autour de la thématique principale plusieurs halos peuvent être circonscrits. Un premier domaine autour de l'« espace » et un second autour du substantif « centre » et un dernier noyaux en haut composé de deux branches autour des sites internet et des systèmes d'information. La thématique de la sécurité constitue ainsi partie de ce dernier élément où se retrouve les substantifs « attaque » et « victime ». Elle constitue également un élément du halo « centre » au travers du substantif « harcèlement ».

B – Résultats à partir de Google News à l'aide de l'agent logiciel GnOSIE⁶⁰⁶.

Corpus n°5 – Cyber Google News GnOSIE FR 2001-2016	
« Ensemble des publications francophones de presse généraliste et spécialisée entre 2001 et 2016 contenant le mot cyberespace ou un terme dérivé sur la base de données de Google News. »	
Date de début : 1^{er} février 2001	
Date de fin : 31 octobre 2016	
Nombre de documents retenus : 20362 sur 45702 résultats pertinents. [Estimation totale du nombre d'articles publiés sur cette période environ 10 600 000 comptabilisés sur ce moteur de recherche, tous sujets confondus]	Nombre d'occurrences de termes « cyber » : 43166 <ul style="list-style-type: none">• 2001 à 2005 (inclus) : 4303• 2006 à 2010 (inclus) : 14532• 2011 à 2016 (inclus) : 24331

Figure 35 – Descriptif du corpus d'étude
« Cyber Google News GnOSIE FR 2001-2016 ».

L'intérêt de ce dernier corpus d'analyse réside principalement dans une tentative de diminué l'impact des « annonces » de journaux observé dans le corpus n°4 et qui a pu expliquer la force relative des cyberbases, cybercafés et autres adjectifs « cyber ». Google News (ou Google Actualités) est un moteur de recherche de Google créé en 2002 qui indexe des articles de presse issus de différents sites Internet. La partie française a été lancée en 2009⁶⁰⁷. La base de données n'est pas propre comme celle de Factiva, mais intègre de façon dynamique les informations de manière algorithmique. Les articles sont triés par degré de pertinence au travers d'une comparaison entre la notoriété d'une source et les articles publiés en même temps sur un

⁶⁰⁶ Pour rappel : l'agent logiciel GnOSIE pour « *Google news Optimization to Study with Iramuteq Environnement* » est un outil codé en JavaScript sous Licence MIT. Il a été créé dans le cadre de cette recherche afin d'automatiser un certain nombre de tâches répétitives et de gagner du temps sur la constitution et la mise en forme des corpus en transformant les flux de données Google News, en texte utilisable par le logiciel Iramuteq. (Cf. Chapitre liminaire)

⁶⁰⁷ Du point de vue du droit d'auteur, les données du moteur de recherche sont sous le régime du Copyright Act des États-Unis d'Amérique qui autorise l'utilisation des données à des fins de recherche. Du point de vue des relations entre Google, la presse française et l'État français, la situation semble clarifiée au terme d'un accord entre l'Agence France Presse et l'entreprise en 2007 ainsi que d'un accord avec l'État français le 1^{er} février 2013.

sujet proche. Il y a donc un effet de tri qui était absent du premier corpus presse. D'un point de vue général, ce corpus permet de mettre en avant une structuration particulière des agrégateurs de presse. Si Factiva était tourné vers les annonces légales, les dépêches locales et les quotidiens régionaux, l'algorithme de Google aura tendance à privilégier la presse spécialisée ainsi que les articles de presse au détriment des petites annonces.

Il s'agit de tendances générales. Des exceptions existent. Beaucoup d'articles sont présents dans les deux corpus. Mais à échelle comparable, la composition des deux corpus s'en trouvera différenciée. L'impact de GnOSIE est relativement neutre sur la constitution du corpus, dans la mesure où le logiciel se contente de formuler des requêtes auprès de Google News, il ne s'occupe pas du tri des données. Du point de vue des résultats et de la structuration du corpus, il y a eu un effet assez inédit : une absence de termes « cyber » dans plus articles identifiés par le moteur de recherche ayant pour objet Internet ou le numérique dans un sens plus large.

Sur les 45702 résultats pertinents identifiés par le moteur de recherche à travers notre agent logiciel GnOSIE complété par une recherche conventionnelle (**Figure 35**), c'est environ 1800 articles qui ont dû être écartés du fait de ne comporter aucune occurrence de termes cibles. Les autres critères de tri ont abouti à des exclusions classiques : Outre, les reprises, les nombreux noms propres, noms d'entreprise ou de marques, retirés les références à la série télévisée *Les experts : Cyber* et d'autres œuvres culturelles ont également dû être retirées.

Enfin d'adopter une logique analogue aux autres corpus, le recensement de toutes les occurrences du terme cyberspace et des termes dérivés se situera en **Figure 36**. Les résultats de la classification hiérarchique descendante (chi 2) seront en **Figures 37 et 38**. Enfin, les **Figures 39 et 40** constitueront le résultat de l'analyse de similitude fondées sur les cooccurrences sans et avec la prise en compte de l'affixe « cyber »

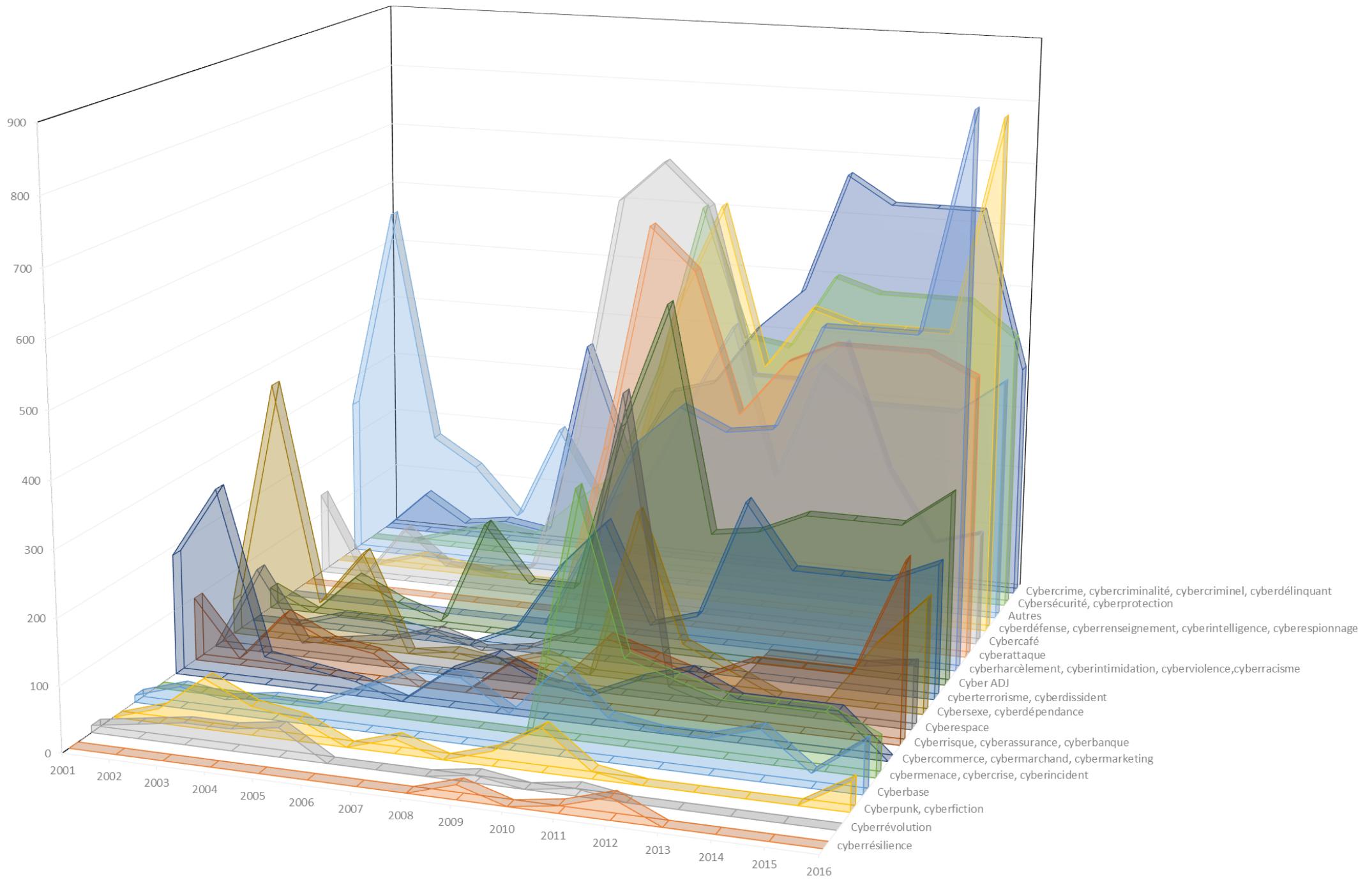


Figure 36 – Recensement des occurrences des termes « cyber ». Corpus n°5

1 – Analyse des résultats du recensement (Corpus 5).

Nous avons identifié 43166 occurrences au sein de ce corpus. 4303 résultats se situent entre 2001 et 2005, 14532 entre 2006 et 2010, 24331 entre 2011 et 2016 (**Figures 35 et 36**). Le corpus semble ainsi suivre un schéma analogue aux autres. Il se distingue toutefois par une certaine brutalité dans l'évolution des termes dominants ainsi que par une recrudescence de thématiques ponctuelles. D'un point de vue thématique, il semble correspondre davantage aux évolutions de l'actualité que le premier corpus de presse. La perspective majeure est celle de la sécurité au détriment de celle de l'accès. On retrouve ainsi le groupe « cybercriminalité » (5049 occurrences) et le groupe « cybersécurité » (4554 occurrences) en tête, suivi par les variations « autres » (4532 occurrences) qui viennent marquer la prolifération du langage qui était soulignée dans nos développements liminaires. La « cyberdéfense » et le groupe « cybercafé » (avec beaucoup d'annonces d'ouvertures) sont autant présent l'un que l'autre (4488 occurrences chacun), suivi par le groupe « cyberharcèlement » (4136 occurrences). Il y a donc un effet similaire au corpus 4 où les formes dominantes du corpus peuvent être réparties entre l'accès à l'information et la sécurité de l'information. La « cyberbase » est moins présente (935 occurrences au total, contre 7393 dans le corpus 4).

Il est possible de tracer une coévolution dans un sens similaire de l'ensemble des termes qui appartiennent à la sécurité de l'information : les groupes « cyberdéfense », « cybercriminalité », « cyberattaque », « cybersécurité », « cybermenace », « cybermenace », « cyberterrorisme » connaissent tous une forte progression autour de l'année 2010 qui vient établir un nouveau seuil d'occurrences pour les groupes en question.

Le corpus 5 se démarque particulièrement car ses évolutions vont ressembler à un reflet caricatural des résultats de l'analyse des discours institutionnels. Avec beaucoup plus de documents, de références, ce corpus produit une thématique similaire qui ne recoupe pas nécessairement les mêmes thèmes mais qui une évolution comparable de groupes clefs : « cyberespace », « cybersécurité », « cybercrime », « autres ».

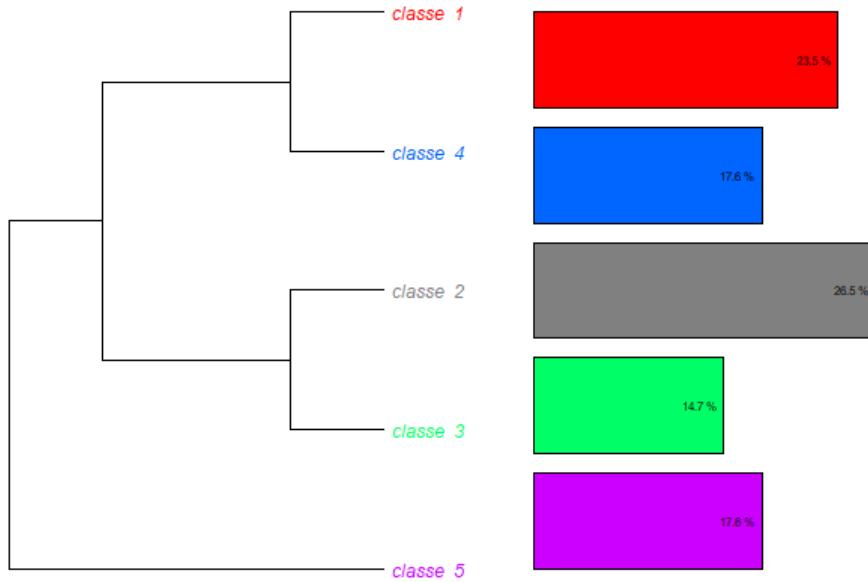


Figure 37 – Chi2 - Classification hiérarchique descendante des segments « cyber ». Corpus n°5

Classe 1 23,53 %		Classe 2 26,47 %		Classe 3 14,71%		Classe 4 17,65%		Classe 5 17,64%	
Sécurité	32.0	Milieu	32.0	Commerce	32.0	Continuité	18.87	Rumeur	26.37
Profiter	32.0	Harcèlement	26.37	Marketing	18.87	Vulnérabilité	14.34	Métier	26.37
Compétence	32.0	Violence	26.37	Avantage	18.87	Déceler	12.31	Dépendre	16.33
Gendarmerie	32.0	Ministère	26.37	Café	14.34	Niveau	12.31	Gouvernance	16.33
Fraude	22.15	Toucher	24.31	Vitesse	14.34	Criminel	9.49	Structure	14.7
Escroc	18.87	Etudiant	23.17	Marchand	14.34	Crime	5.74	Réputation	11.82

Figure 38 – Chi2 - Formes les plus représentatives de chaque classe (en chi2). Corpus n°5

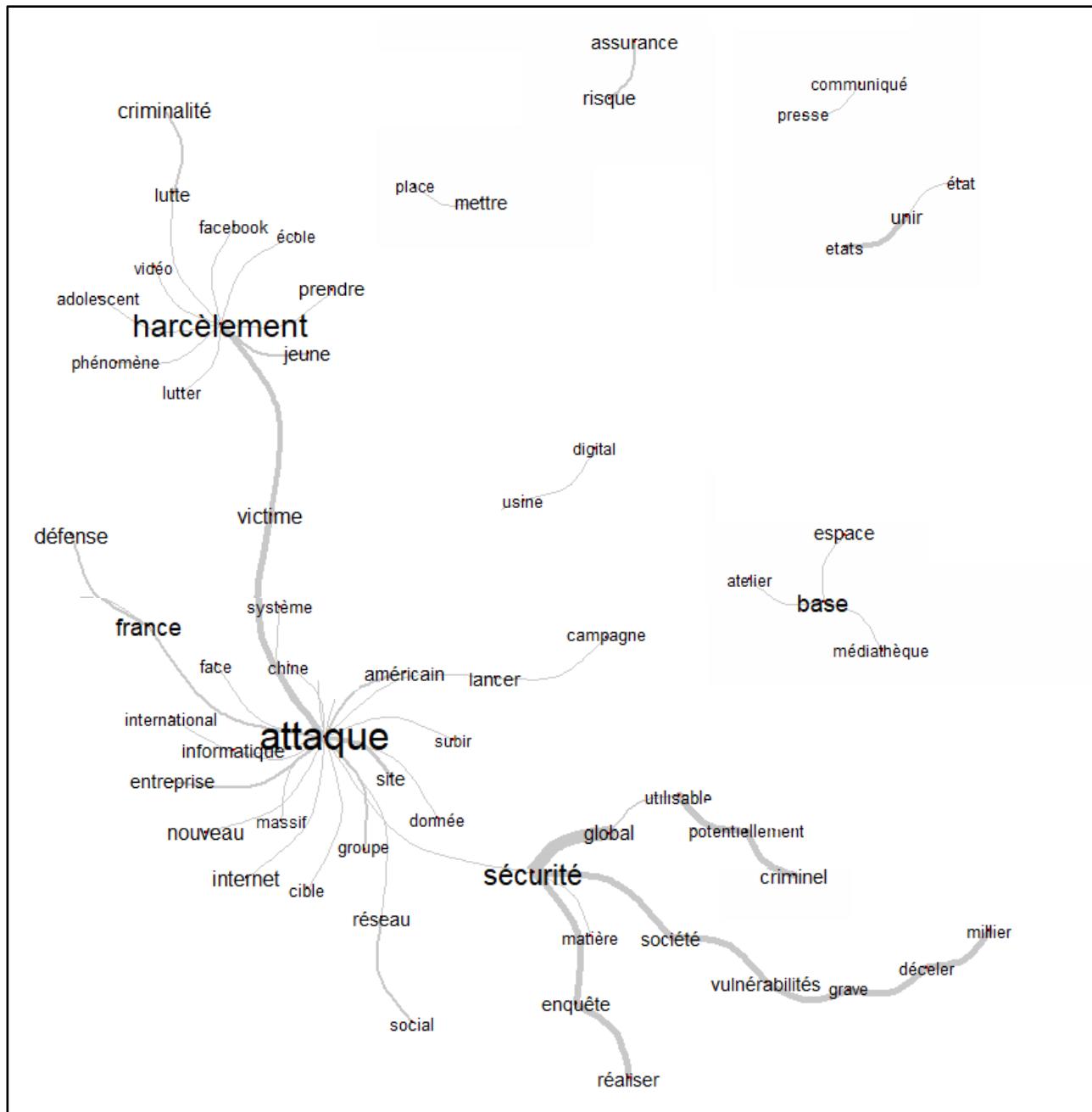


Figure 39 – Analyse de similitude en l'absence des termes « cyber ». Corpus n°5

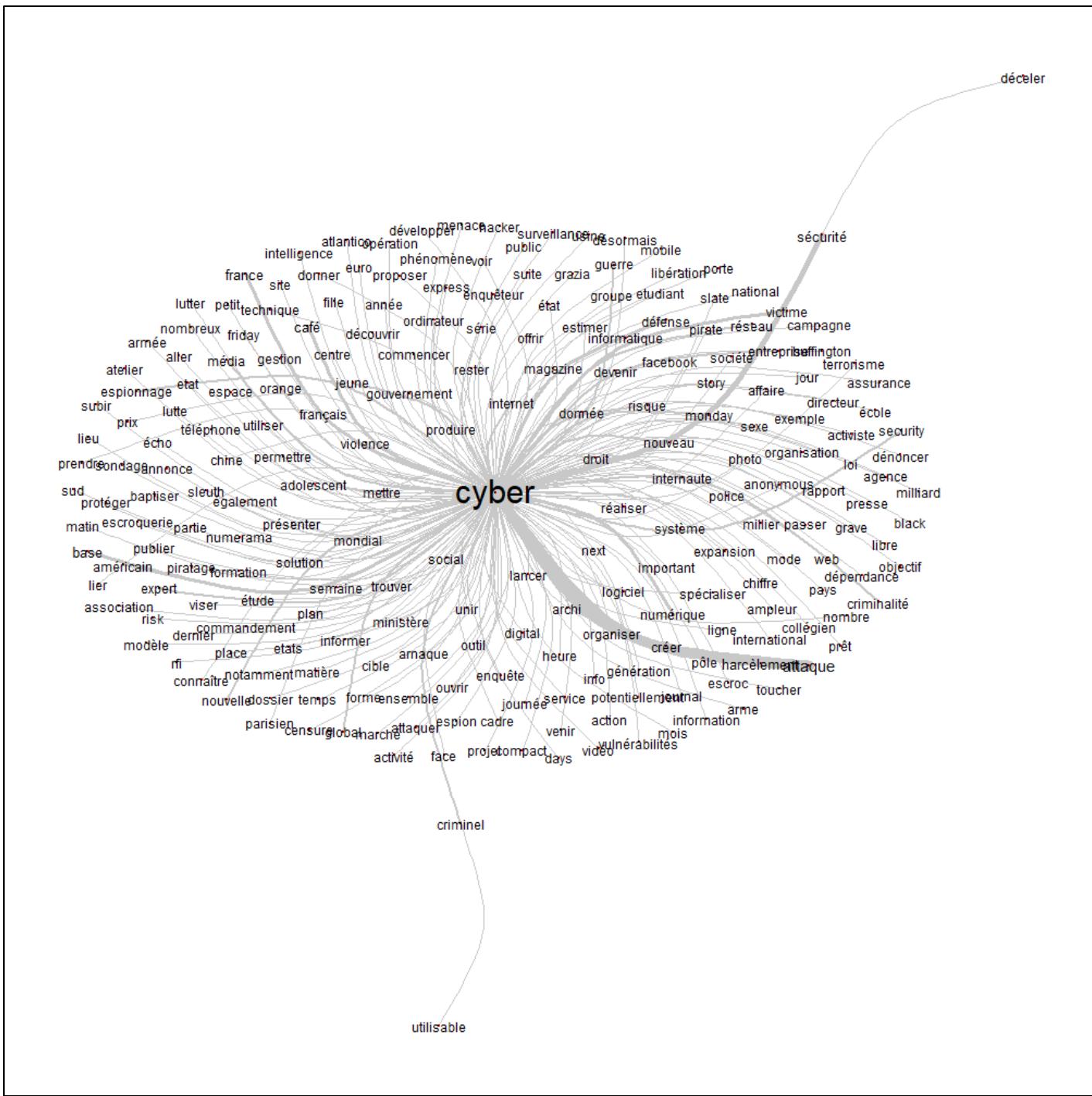


Figure 40 – Analyse de similitude à partir des termes « cyber ». Corpus n°5

2 – Résultats des approches thématiques : mondes lexicaux et analyse de similitude (Corpus 5)

Au terme de la classification hiérarchique descendante (**Figures 37 et 38**), les classes identifiées sont :

- La classe 1 (23,53 % du corpus) qui concerne la sécurité de l'information de manière générale dans la vie quotidienne, dont les substantifs les plus représentatifs sont : « Sécurité », « Profiter », « Compétence », « Gendarmerie », « Fraude », « Escroc ».
- La classe 2 (26,47 % du corpus) qui est concentrée sur la violence morale dans le milieu scolaire et étudiant. « Milieu », « Harcèlement », « Violence », « Ministère », « Toucher », « Etudiant ».
- La classe 3 (14,71% du corpus) qui se focalise sur les aspects commerciaux : « commerce », « marketing », « avantage », « café », « vitesse », « mercatique » (très présent au début des années 2000). Il s'agit de la classe la moins présente.
- Les classes 4 et 5 (17,65% et 17,64% du corpus) sont deux classes une nouvelle fois consacrées à certains aspects de la sécurité de l'information : d'une part sur les enjeux systémiques de l'exploitation des vulnérabilités ; d'autre part, principalement sur les questions de rumeur, de réputation, de dépendance et de gouvernance de l'information.

Contrairement au corpus 4, la sécurité revient comme thématique principale du corpus (4 classes sur 5 peuvent y être reliés). La place des victimes semble importante. Le dernier enjeu semble moins être l'accès à l'information en lui-même que la création et la bonne gestion des entreprises. C'est cohérent avec le caractère de presse spécialisée d'une partie des sources et le rejet des annonces. Parmi les thématiques communes, les deux corpus de presse accordent une place particulière à la criminalité, à la défense, au harcèlement, à l'emploi et à l'ouverture de cybercafé. L'individu est au cœur des enjeux soulevés par les articles de presse. La dimension collective existe dans l'inter-individualité sinon à une échelle locale ou sectorielle.

Les analyses de similitude (**Figures 39 et 40**) mettent en avant l'aspect sécuritaire de l'utilisation du terme cible et de ses variations. Les trois plus gros liens des termes « cyber » sont établis avec l'« attaque », le « harcèlement », et la « sécurité ». Ces trois nœuds sont interconnectés. Deux nœuds semblent intéressants : le nœud « base », qui établit un lien avec

le corpus 4 et la question des lieux d'accès à l'information, et le nœud « unir » qui fait apparaître la dimension internationale. De manière générale, une dysmétrie apparaît dans la cooccurrence des différents nœuds. Les liens de cooccurrences sont les plus forts sur le nœud « sécurité », de même que le lien entre « attaque » et « harcèlement » au travers du terme de « victime ».

L'acteur régional « France » entretient un lien fort avec les termes de « défense » et d'« attaque ». Cela pourrait vouloir dire que l'État intervient dans l'actualité à un niveau politique soit comme victime d'une « attaque » et qu'il y répond de façon majoritaire par la « défense » ou du moins qu'il s'agit du secteur d'intervention le plus apparent dans les médias. Ce qui n'est pas non plus incohérent au regard de l'observation participante conduite sur le terrain et de la veille réalisée au profit de cette thèse. C'est également assez cohérent avec les résultats des analyses des discours institutionnels.

Les deux corpus analysés pour comprendre cette utilisation du phénomène « cyber » dans la presse montre une utilisation majoritaire du cyberspace afin de créer des mots nouveaux pour décrire l'information dans les questions relatives à son accès (principalement sous l'angle de la médiation et de l'entreprise), ainsi que de la sécurité (comprise comme partiellement criminalisée mais qui intègre aussi des situations de harcèlement comme le corpus 3). La thématique de la sécurité est très présente dans les articles de presse et assez peu dans les annonces. Les deux corpus montrent également une importance des « autres » termes illustrant l'importance de la prolifération d'un lexique des variations « cyber » ainsi que son importante hétérogénéité.

Parmi ces variations, la sécurité est un enjeu qui se dégage tout particulièrement. En tant que discours de sécurité, le discours « cyber » de la presse sera toutefois spécifique en ce qu'il se destine à un public généraliste. L'analyse de discours appliquée à la presse ne permet pas nécessairement de préciser le cyberspace, mais d'établir les traits de caractères dominants de l'individu en interaction avec celui-ci.

Section 3 - Eléments de discussion du phénomène discursif « cyber ».

Au terme de notre analyse, 83715 utilisations du cyberspace ou d'un terme dérivé ont été observées (dont 4055 dans les discours institutionnels). Schématiquement, sur notre période d'analyse entre le 1^{er} février 2001 et le 31 octobre 2016, cela équivaudrait à un peu plus de 14 occurrences par jour. Toutefois, la répartition de ces occurrences est inégale. Si nous devions

donner une valeur identique à chacun des corpus peu importe le nombre d'occurrences, la moyenne relative des résultats situés entre 2011 et 2016 correspondrait à 74,64 % des résultats obtenus (entre 56,37% et 89,06%). En moyenne, 25,36% des résultats seulement se trouveraient donc entre 2001 et 2011, ce qui illustre un accroissement du phénomène linguistique observé. Les deux catégories de corpus objets de cette analyse décrivent un discours où la sécurité est un paradigme dominant. Toutefois ce phénomène en tant que tel est loin d'être univoque. L'objectif étaient de déterminer les traits dominants à partir de la recherche de résultats en fréquences et cooccurrences des termes⁶⁰⁸. Au-delà de fournir un regard thématique sur l'objet « cyber », il s'agissait ici, par la statistique, de regarder son contexte et son objet d'utilisation au sein des différents textes mis en perspectives au sein des différents corpus. Avec son introduction progressive dans les discours institutionnels, ce terme semble s'être peu à peu doté d'un nouvel ensemble de significations tournées vers la sécurité et devenant peu à peu majoritaire. Plusieurs traits peuvent être déduits concernant notre objet d'étude.

Utiliser un terme composé du mot « cyber » revient pour une institution à parler de sécurité, et à rapporter cette sécurité à l'information comprise comme informatisée. Cette situation s'accroît dans le temps quel que soit le niveau de dialogue considéré. Cette thématique sécuritaire supplante totalement les autres thématiques considérées : libertés, accès à internet, gouvernement ouvert, transformation numérique de l'administration, enjeux des macro-données... Le cyberspace en tant que notion participe ainsi de la définition d'un enjeu de sécurité par la définition d'une menace et d'une valeur de référence qui est la sécurité du système informatique. Cette valeur se transforme pour quitter l'idée de sécurité et aller vers une idée de résilience. Déjà pleinement consacrée à l'échelle internationale depuis 2010, elle peine à devenir majoritaire à l'échelon national français.

La politique française en matière de sécurité de l'information semble fortement intégrée à un niveau régional. Si l'approche de l'ONU semble aller dans ce sens à la lecture des passages concernés, l'Union Européenne semble quant-à-elle davantage intégrative bien que l'État demeure l'intervenant principal. Il est important de souligner l'omniprésence de la criminalité parmi les résultats qui en matière de sécurité de l'information semble hiérarchiser les préoccupations régionales comme étant d'abord liées à des missions « de police » avant d'être

⁶⁰⁸ Héritière de la linguistique anglosaxonne, une cooccurrence se comprend comme une présence simultanée de deux mots dans le même énoncé. Le concept de cooccurrence est en sciences linguistiques le fondement du champ lexical ou de la thématique (isotopie)

des « missions militaires ». L'aspect « militaire » tient d'ailleurs une place un peu particulière dans les résultats. Du point de vue du langage, la tendance entre 2001 et 2016 ne serait pas tant un phénomène de sécularisation du militaire, mais plutôt une forme de consécration de la logique inverse. Il y a ici une forme de paradoxe alors que la cyberdéfense est « érigée au rang de priorité nationale » par le Livre blanc pour la défense et la sécurité nationale de 2013. De plus, en France, la majeure partie des publications officielles importantes consacrées au cyberspace qui emportent des dispositions contraignantes sur la période considérée sont des sources dont la vocation première est « militaire » : livre blanc sur la défense et la sécurité nationale, la loi de programmation militaire...

A la lumière des résultats de cette analyse, ce qui pourrait sembler paradoxal interroge la compréhension de la sécurité entre approches classiques et approches critiques. Si les origines complexes des conflits contemporains amènent à élargir le champ de la sécurité au-delà de la sécurité étatique à travers considérations environnementales, sociétales ou économiques. La sécurité de l'information implique davantage une approche holiste de la sécurité qui rejette toute segmentation de ce champ. Bien que réduisant les aspects de défense, la sécurité de l'information restituerait ainsi le rôle de l'État dans une conception élargie de la sécurité, et diffuse celle-ci aux autres acteurs de la société. Cette sécurité de l'information comprise de manière globale est située au carrefour des niveaux infra-étatiques et supra-étatique, dans tous les secteurs. Loin de l'isoler, la sécurité de l'information entraîne ainsi un accroissement des échanges entre l'acteurs régional et l'ensemble des acteurs de la société civile. La réorientation des moyens au sein et à l'extérieur d'un acteur pour prendre en compte un nouvel élément de l'environnement conflictuel entretient nécessairement une relation complexe avec la représentation que l'acteur se fait de sa propre sécurité.

Cette conception de la sécurité, organisée de façon réticulaire, trouve en France trois exemples de dispositifs (plutôt sur la fin de la période considérée). Tout d'abord, en Bretagne, la création du Pôle d'excellence Cyber qui regroupe les écoles militaires, universités, centres de recherche et entreprises dont l'activité est liée au domaine des nouvelles technologies de

l'information et de la communication. La réserve citoyenne de cyberdéfense (RCC)⁶⁰⁹, et enfin à l'image de nombreux autres États, la création des opérateurs d'importance vitale (OIV)⁶¹⁰.

La place de l'acteur régional est consacrée face à un enjeu de sécurité compris de manière plus globale. L'État constitue ainsi l'échelon prioritaire d'intervention, y compris du point de vue de l'international. Les deux angles de compréhension majeurs de cette sécurité sont : la menace criminelle, ou la sécurité des systèmes elle-même. La résilience ou la défense ne constituent que des thèmes secondaires importants qui n'existent au premier plan du discours qu'à un seul niveau institutionnel donné (l'ONU pour la première, l'État pour la seconde). Les libertés individuelles et la protection des droits subjectifs est principalement porté par les acteurs supra-étatiques. Plus, on s'éloigne de cette dimension étatique régionale, plus les intérêts particuliers des citoyens sont un enjeu important.

Le caractère d'extranéité d'un certain nombre de situations semble être un élément d'importance impliquant une insistance sur les aspects transnationaux (des flux, des menaces...) Corolairement, l'idée « spatiale » qui ferait que le cyberspace est avant tout un espace n'est présente que dans la différenciation. Le cyberspace n'est pas homogène, universel et dépourvu de frontières.

Ce discours sur la sécurité de l'information met avant une position particulière de l'acteur régional, des mécaniques symboliques particulières et opère une discrimination des enjeux dans l'ensemble plus large des sujets concernant le numérique. Nous terminerons par quelques éléments critiques contenus dans le discours et qui permettent d'en nuancer la réelle portée.

⁶⁰⁹ La RCC a pour objectif de sensibiliser la Nation aux enjeux de la cyberdéfense. « A ce titre, elle crée un lien avec les citoyens, et en particulier avec les acteurs économiques et industriels, qu'ils soient de grands groupes ou des PME/PMI, les relais d'opinion, les think-tanks, les milieux universitaires et la représentation nationale ».

⁶¹⁰ Depuis 2006, se développe un statut particulier nommé « opérateur d'importance vitale » (OIV). Aujourd'hui, ce statut est consacré par la fameuse Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 (LPM) et portant diverses dispositions concernant la défense et la sécurité nationale. Et il est défini par les articles L 1332-1 et L 1332-2 et L 1332-6-1 à L 1332-7 du Code de la défense. Il fait intervenir deux éléments essentiels que sont l'opérateur et le secteur. Au sens du Code de la Défense, le secteur d'importance vitale (ou SAIV) concerne les activités qui ont trait à la production et la distribution de biens ou de services indispensables (dès lors que ces activités sont difficilement substituables ou remplaçables) : à la satisfaction des besoins essentiels pour la vie des populations ; à l'exercice de l'autorité de l'État ; fonctionnement de l'économie ; au maintien du potentiel de défense ; ou à la sécurité de la Nation ; ainsi que les installations classées pour la protection de l'Environnement (ICPE –L 511-1 du Code de l'Environnement) ou comportant une installation nucléaire de base, dont la destruction ou l'avarié peut présenter « un danger grave pour la nation ».

A – Une vie internationale mésestimée au profit d'une position privilégiée de l'acteur régalien dans le discours.

La grande question soulevée par les résultats est celle d'une spécificité de l'acteur régalien dans le discours. Ainsi l'idée de privilège n'entend pas ici qualifier un avantage quelconque dans la position de l'État mais un statut particulier. Comme nous le soulignions au moment d'évoquer les résultats de notre enquête sur les discours institutionnels, l'État constitue l'échelon d'intervention prioritaire pour traiter la question de la sécurité de l'information, y compris du point de vue de l'international. Cette question est également présente dans les corpus de presse. L'idée d'une position privilégiée de l'acteur régalien dans le discours vient avec l'idée d'une vie internationale balbutiante. Une seconde version de cette idée consiste à dire que bien qu'une vie internationale existe, elle est réduite à sa plus simple expression : « on en parle beaucoup »⁶¹¹. C'est une idée que nous avons déjà commencé à nuancer, mais nous allons nous y attarder davantage notamment à la lumière des résultats obtenus. En effet, contrairement à cette idée reçue relativement bien admise, le phénomène semble plus présent en termes d'occurrences à l'international qu'au niveau national. La discours sur la sécurité de l'information oppose l'idée une réponse nationale à une menace transnationale. Toutefois, les résultats obtenus à partir de nos corpus 2 et 3 mettent en avant de nombreuses spécificités dans leur articulation.

La spécificité régaliennes en matière de sécurité de l'information se définit premièrement dans un rapport d'exclusivité à un certain nombre de thématiques. D'une part, il existe des thématiques où l'ensemble du discours en fait l'acteur principal (cybercriminalité). Il existe des thématiques où l'État possède une forme de monopole (défense) qui sont non-évoqués par les autres acteurs ou de manière marginale. Par ailleurs, la production de l'État (Corpus 1) se met à part des autres corpus en ne recherchant que peu l'intérêt de l'échelon individuel qui est évoqué par l'ensemble des autres corpus à la fois d'un fois de vue supra-étatique et d'un point de vue infra-étatique.

⁶¹¹ Première remarque sur le phénomène cyberspace tirée d'un entretien conduit le 9 juin 2015 avec le directeur adjoint des affaires stratégiques, de sécurité et du désarmement de la direction générale des affaires politiques et de sécurité du Ministères des affaires étrangères (entretien semi-directif réalisé au cours d'un déjeuner au café Le Pierrot, Avenue de la Motte-Picquet, Paris.)

1 – L’État comme acteur principal pour lutter contre la menace « transnationale » de la cybercriminalité.

La cybercriminalité constitue avec la cybersécurité le principal terrain de médiation autour des problématiques de sécurité de l’information. C’est par cette thématique que les acteurs interviennent principalement auprès de l’acteur régional et c’est l’une des thématiques partagées entre tous les acteurs. Elle se situe au cœur du dialogue de l’État avec les autres acteurs et représente une forme de frontière coupant le discours en deux ensembles : ce qui intéresse prioritairement l’État et ce qui intéresse tout le monde.

La cybercriminalité incarne la figure de la menace principale de l’informatique ainsi qu’une grande partie de sa représentation mystique : l’absence de frontières, l’image d’Épinal du détenteur de la connaissance informatique, la possibilité d’un rapport de force inversé par rapport au monde réel. L’action criminelle figure également à la base de l’invention du cyberespace dans une littérature de science-fiction qui puise ses racines dans les histoires policières et le roman noir. La nouvelle *Burning chrome* de 1982 ne raconte-telle pas l’histoire de deux voleurs cherchant à s’emparer de la connaissance humaine à travers l’informatique ? Il est donc logique que cette figure du criminel soit l’un des principaux développements théoriques issus de la notion littéraire. Paradoxalement, c’est également l’une des subdivisions les plus construites car c’est l’une des seules composantes du cyberespace à pouvoir bénéficier des dispositions d’un traité international multilatéral : la *Convention de Budapest sur la cybercriminalité*, rédigée en 2001 par le Conseil de l’Europe avec les États-Unis, le Canada, le Japon et l’Afrique du Sud, et entrée en vigueur le 1^{er} juillet 2004. Même si, les propositions contenant un mot composé en « cyber » sont réservées aux principes plutôt qu’aux dispositions applicables. La cybercriminalité est traitée de façon similaire dans les discours institutionnels. L’idée de criminalité est systématiquement associée à l’idée de lutte et à l’idée de convention du fait du texte précité. Il est intéressant de constater que chaque niveau considéré semble avoir une vision particulière de la sécurité, là où leurs visions de la criminalité semble s’aligner au moins d’un point de vue du langage.

Tout acteur menaçant sera la plupart du temps un « cybercriminel ». Ce « cybercriminel » est un terme large qui a la propriété d’englober toutes les formes d’adversaires : terroristes, mafias, escrocs, trafiquants, espions industriels, hackers, maîtres-chanteurs, individus téléchargeant des fichiers en infraction avec le droit d’auteur, utilisateur

de réseaux sociaux ayant des propos inappropriés... Toutes ces personnes peuvent faire l'objet du qualificatif à raison de leur utilisation de l'informatique dans le cadre de leurs activités illégales ordinaires, ou à raison d'un mauvais usage de l'informatique. Les deux seules exceptions que la cybercriminalité ne semble pas couvrir est la négligence des utilisateurs (y compris lorsque celle-ci est en infraction avec une obligation légale de protection) et des faits imputables aux autres États.

La cybercriminalité permet de qualifier les auteurs des infractions retenus comme des cybercriminels : pourtant la plus grande partie des comportements susceptibles de se voir inclut au chapitre de la cybercriminalité constituent des délits et non des crimes⁶¹². Il y a une forme d'aggravation dans le langage utilisé pour décrire la réalité des infractions commises. Cela est particulièrement le cas lorsque l'on se trouve dans la presse (Corpus 4 et 5). Par ailleurs, si la criminalité possède une dimension de menace transnationale à l'instar des discours sur le terrorisme, la piraterie, le trafic de drogue, son traitement demeure profondément ancré dans chacun des États qui demeurent l'échelon prioritaire pour lutter contre celle-ci, y compris lorsque les cybercriminels sont situés à l'étranger. C'est notamment la raison pour laquelle la société internationale voit émerger des réseaux de coopération internationale⁶¹³. Le fondement de cybercrime n'est donc pas à rechercher du point de vue la loi qui le qualifie pour comprendre son développement dans le discours. Dupoint de vue de ce discours, le crime⁶¹⁴ aidé ou rendu possible par l'informatique se caractérise essentiellement par une double présomption de technicité du phénomène et d'extranéité. Les forces de l'ordre sont réputées être aux antipodes du cybercrime. Les forces de l'ordre sont traditionnellement conçues pour lutter contre les crimes à faible volume et à fort impact dans un contexte national. Tandis que le cybercrime repose sur un fort volume et un faible impact dans un contexte international⁶¹⁵. Quand on parle de cybercriminalité, il faut donc articuler trois langages spécialisés différents : le langage « cyber » qui décrit l'enjeu politique en tant que composante de la « cybersécurité », le langage « technique » souvent en anglais qui décrit les instruments et pratiques possibles, le langage

⁶¹² Voir notamment la *Convention de Budapest sur la cybercriminalité* évoquée plus haut.

⁶¹³ DUPONT Benoît,, « La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale », *Cultures & Conflits*, 2016/2 (n° 102), pp. 95 – 120.

⁶¹⁴ Chez Emile Durkheim le crime se comprend comme « tout acte qui, à un degré quelconque, détermine contre son auteur cette réaction caractéristique qu'on nomme la peine » voir. DURKHEIM Emile, *De la Division du travail social*, Librairie Félix Alcan, 1893, p. 173.

⁶¹⁵ DUPONT, op-cit. pp. 95-96

pénal « classique » qui caractérise des pratiques et établit des infractions (au sein duquel il faut distinguer entre l'ensemble des qualifications possibles avec l'ensemble des acteurs possibles...).

Ce caractère extraordinaire de la cybercriminalité conduit les acteurs supra-étatiques à militer pour une harmonisation législative entre les États. Si on garde l'exemple de la *Convention de Budapest*, cette harmonisation des législations (et des procédures) figure parmi les objectifs principaux du document avec l'amélioration de la coopération. Les acteurs infra-étatiques se concentreraient sur la logique des moyens alloués à la lutte contre la cybercriminalité : à la fois par les forces de l'ordre mais aussi dans les autres composantes de l'État jusqu'aux hautes autorités chercher de réguler l'ensemble du numérique (concurrence, droits intellectuels, libertés...). C'est l'un des points de fracture entre le discours et la réalité de la coopération internationale sur lequel il nous faudra revenir. Sur le volet prévention du cybercrime, c'est également l'État qui est le principal garant de l'ensemble des bonnes pratiques et des certifications qui attestent d'un niveau suffisant ou non. En France, c'est le rôle de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) créée en 2009. En Allemagne, c'est le rôle de l'office fédéral de la sécurité des technologies de l'information (BSI⁶¹⁶)... L'ensemble des services mentionnés peut être placé sous l'autorité des ministères de l'intérieur respectifs des États concernés soit directement sous la responsabilité du chef du gouvernement de l'État en question. Toutefois, des travaux existent au niveau européen pour des certifications communes notamment par le biais de l'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). L'OTAN est également concerné ici à travers son centre d'excellence basé à Tallinn.

2 – Une spécificité normative « réservée à l'État » : la défense comme domaine régalien.

Outre ce rôle de premier plan accordé à l'acteur régalien dans la lutte contre la cybercriminalité, l'État est également une source concernant la défense. Non seulement, il s'agit d'un domaine prioritaire, mais il est relativement marginal sinon absent de la plupart des corpus supra-étatiques. Les corpus presse, quant-à-eux, se contentent d'informer de l'action de l'État dans ce domaine précis. En effet, de nombreux articles de presse soulignent l'action de l'État en matière de défense qui est sans doute l'une des branches de l'État qui communique le plus

⁶¹⁶ BSI : *Bundesamt für Sicherheit in der Informationstechnik*.

sur son activité en la matière. La thématique de la défense apparaît dans la production normative de l’Union Européenne comme relativement secondaire (ce qui s’explique par la place particulière de la défense en matière de coopération). Au niveau européen, la dimension « défense » concentre sa présence en dehors des thèmes principaux entre les années 2013 et 2015 où de nombreux textes sont pris pour ériger la cybersécurité au rang d’enjeu. Au-delà de l’effort d’intégration de la cyberdéfense dans les stratégies nationales, la dimension défense européenne se cantonne ici à la coopération dans le cadre de le PSDC et à la protection des infrastructures de l’Union. La thématique de la défense (ainsi que de la « cyberdéfense ») est en revanche absente de la production de l’Organisation des Nations Unies. Cela s’explique par l’absence de la thématique « défense » dans le langage de l’ONU qui s’exprime davantage en termes de « maintien de la paix » et de « sécurité collective ». Ce dernier tropisme marque d’ailleurs le thème de la sécurité du point de vue de l’analyse du discours (corpus 3).

Jadis présenté comme la première thématique en termes d’importance entre 2006 et 2010, la cyberdéfense est devenue une priorité « secondaire » du discours par rapport à la cybersécurité. Toutefois, elle représente en réalité le plus fort octroi de moyens à tous les niveaux. Du point de vue étatique, la cyberdéfense représente les plus grosses créations de postes dans l’administration après les décentralisations. Encore aujourd’hui, la plupart des augmentations du budget du ministère de la défense ou des armées comprennent un volet « cyber ». Au niveau infra-étatique, les créations d’entreprise en cyberdéfense continuent de croître. Au niveau supra-étatique, il existe un fort consensus autour du fait que la défense relève du domaine de l’État.

D’après l’analyse des discours institutionnels, la défense n’existerait donc pas dans la « Cité » pour ce qui relève de l’information parmi les enjeux de sécurité mais existerait comme un élément un peu à part de celle-ci, contrairement aux menaces qui sont regardées comme multisectorielles et implique l’intervention d’autres acteurs que ceux de la défense. Il y a ici une autre forme de paradoxe alors que la cyberdéfense est « érigée au rang de priorité nationale » par le Livre blanc pour la défense et la sécurité nationale de 2013 (et celui de 2008 pour les systèmes d’information). Comme il a déjà été souligné, la majeure partie des publications officielles importantes consacrées au cyberspace qui emportent des dispositions contraignantes sur la période considérée sont des sources dont la vocation première est « militaire » : livre blanc sur la défense et la sécurité nationale, la loi de programmation militaire…

Du point de vue du fond, le volet « cyberdéfense » se conçoit de façon différente du volet « cybercriminalité ». Derrière l'idée de cyberdéfense, la sécurité nationale trouve à s'appliquer. Il y a donc une différence téléologique entre les deux aspects qui commande une distinction de moyens. La représentation de la menace s'y conçoit comme le sabotage des structures et systèmes qui permettent le contrôle d'un État. La cyberdéfense s'exprime ainsi en termes de lutte informatique pour défendre et attaquer ces systèmes. Cette défense est organisée sous forme de réseau. Depuis 2006, un statut particulier se développe en France, nommé « opérateur d'importance vitale » (OIV). Aujourd'hui, ce statut est consacré par la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 (LPM) et portant diverses dispositions concernant la défense et la sécurité nationale⁶¹⁷. Ce dispositif est recensé dans notre corpus 1.

Il fait intervenir deux éléments essentiels que sont l'opérateur et le secteur. Au sens du code de la défense, le secteur d'importance vitale (ou SAIV) concerne les activités qui ont trait à la production et la distribution de biens ou de services indispensables (dès lors que ces activités sont difficilement substituables ou remplaçables) ; soit ceux correspondant à la satisfaction des besoins essentiels pour la vie des populations ; à l'exercice de l'autorité de l'État ; au fonctionnement de l'économie ; au maintien du potentiel de défense ; à la sécurité de la Nation ; aux installations classées pour la protection de l'environnement⁶¹⁸ ou comportant une installation nucléaire de base, dont la destruction ou l'avarie peut présenter « un danger grave pour la nation ».

Un opérateur d'importance vitale est une organisation qui exerce des activités comprises dans un secteur d'activités d'importance vitale, ou gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement : d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ; ou de mettre gravement en cause la santé ou la vie de la population. Il existe aujourd'hui environ 200 OIV, dont 80 situés dans le secteur public. La liste étant classifiée, les opérateurs d'importance vitale ne sont pas connus du grand public

⁶¹⁷ Il est codifié dans les articles L. 1332-1, L. 1332-2, L. 1332-6-1 à L. 1332-7 du code de la défense.

⁶¹⁸ Au sens de l'article L. 511-1 du code de l'environnement

sauf à se dévoiler de temps en temps lors d'une affaire judiciaire. L'arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs repris par un arrêté du 3 juillet 2008, nous donne néanmoins la liste des douze secteurs concernés. Ces opérateurs se voient attribuer certaines obligations⁶¹⁹. Les OIV doivent donc respecter les mesures de sécurité élaborées par le Premier ministre et soumettre leur système d'information aux audits. Enfin, en matière de cybersécurité, les décrets n°2015-351 et n°2015-350 du 27 mars 2015 fixent les standards en matière de sécurité des systèmes d'information des opérateurs d'importance vitale et notamment la certification des outils permettant d'assurer cette sécurité. Ce dispositif s'est appuyé sur une mise en place sectorielle.

Ces dispositions consacrent de manière réticulaire des relations véritablement organiques entre l'appareil étatique et les opérateurs qui viennent contredire ce discours en faveur d'un cyberespace comme monopole étatique. La performance ne dépend pas alors de l'existence et de la seule action de l'acteur régional mais bel et bien de l'action et de la diligence des personnes qu'il va désigner comme opérateur. Au travers du « cyber », ce n'est plus la seule organisation régionale qui doit assurer la défense ; au contraire son existence même est conditionnée à la diligence d'acteurs asymétriques membre du « réseau » à garantir leurs propres existences par la protection de l'information. Toutefois, ce renversement n'est envisageable qu'à l'aune de la définition d'une sécurité effective, accessible et respectée. Ce qui est loin d'être le cas en pratique et dénature véritablement la doctrine dans son application en matière de cybersécurité. Il apparait donc que les infrastructures de l'État sont mieux protégées que celles de certains OIV privés, y compris dans le secteur de la cybersécurité.

Du point de la coopération internationale, une fois mentionnées les deux limites soulevées pour la cybercriminalité : outils non adaptés (ici, les armées) et nécessité d'harmonisation entre des ensembles politiques qui ont des manières trop différentes d'opérer. Il reste une dernière série de limites qui est intéressante à mentionner : le manque de confiance et le postulat de la volonté de préserver sa souveraineté nationale.

⁶¹⁹ La loi de programmation militaire 2014-2019 sanctionne les manquements (intentionnels ou non) à la loi d'une amende de 150.000€ (donc 750.000€ pour les personnes morales).

3 – L’absence relative de l’individu des centres d’intérêt de l’État : spécificité régaliennes ou spécificité française ?

La concentration de la production institutionnelle du corpus 1 sur un petit nombre de thématiques exclut un certain nombre d’enjeux du discours. Cette exclusion renforce l’idée d’une spécificité régaliennes des thématiques de la sécurité de l’information. Là où ces enjeux apparaissent dans l’ensemble des autres corpus (presse comme supra-nationaux). Ces enjeux concernent principalement l’individu en interaction avec la société. Autrement dit, il s’agira d’interroger le caractère exclusif d’un niveau interindividuel.

La question de l’individu n’est pas nouvelle dans ce chapitre. Au niveau des corpus 2 et 3, elle représentait une forme de préoccupation pour les intérêts et libertés des populations. Au niveau des corpus 4 et 5, les préoccupations étaient davantage tournées vers les dispositifs d’accès à Internet en termes de navigation comme d’entrepreneuriat et les atteintes subies directement par les personnes. Ces centres d’intérêt s’inscrivent dans une perspective téléologique, l’individu, compris comme un groupe plus ou moins restreint, constitue une composante de l’objectif de chacune des organisations productrices du contenu analysé. L’individu-utilisateur a donc un rôle téléologique dans l’argumentation. L’individu abstrait est généralement perçu comme l’acteur qui dérange l’idée de sécurité : Si l’individu travaille pour l’État, il est « à former » ou peut commettre des erreurs. S’il ne travaille pas pour l’État, il est potentiellement menaçant. La remise en cause du paradigme technique qui conditionne la compréhension de la sécurité de l’information ne vient pas atténuer ce point de vue. L’idée dominante dit que l’erreur humaine est à la base de 75 % (Ou 80% en fonction de l’interlocuteur) des problèmes de sécurité informatique. C’est vrai dans le domaine de l’administration, mais aussi dans le domaine de l’entreprise. Il y a donc une préoccupation forte autour de l’individu de la plupart des acteurs mais qui exclue le domaine des grandes publications officielles⁶²⁰.

L’État n’a-t-il aucun rôle à accorder à l’individu dans sa production normative ? Pas vraiment, l’individu est presque totalement absent de la production normative analysée qui ne comprends que ce qui est publié au journal officiel. La réponse tient avant tout à une forme de particularisme culturel. L’État français considère en effet que le sujet de la « cybersécurité » est

⁶²⁰ WEBER Claude, PERROTTET Jean-Philippe, « La place de l’homme dans les enjeux de cybersécurité », op-cit.

de son domaine et envisage ce domaine comme exclusif⁶²¹. Pendant la plus grande partie de la période analysée, l'acteur n'opère d'extension du sujet que par à-coup jusqu'à consacrer le sujet comme relevant d'un intérêt citoyen en 2014. La logique de l'OIV participe de ce mode de raisonnement particulier. Ce n'est que parce que l'État est garant de la sécurité de la population qu'il étend les frontières de sa politique en matière de sécurité de l'information. L'absence de l'individu signifierait ainsi que l'acteur régional se vise d'abord sa propre réforme par sa production normative. Les différents rapports produits à intervalle régulier par les deux chambres du parlement (exclus des journaux officiels) semblent aller dans ce sens⁶²². La priorité en termes d'acteurs se concentre principalement sur l'État et les entreprises.

Du point de vue du discours, d'autres États utilisant l'expression « cyberspace » ou des termes dérivés dans leurs langues respectives inscrivent la priorité de la protection des droits des citoyens de façon assez tardive dans leur production légale : le Japon et les États-Unis d'Amérique en 2013, la Chine et le Royaume-Uni en 2016⁶²³. D'ordinaire, des thématiques tels que la protection des données personnelles ou l'accès à l'information sont traités par d'autres discours que celui marqué par l'usage des expressions en « cyber ».

Moins qu'une exclusion volontaire de l'individu et des aspects plus ou moins centrés sur l'État de telle ou telle politique nationale, l'absence relative de l'individu dans la production normative nationale confère davantage à une forme de structuration du discours autour d'une discrimination des enjeux.

B – Discrimination des enjeux politiques de l'information : les enjeux portés par le discours « cyber ».

Les résultats de l'analyse nous permettent de construire une typologie des enjeux selon leur degré d'importance dans la sécurité de l'information. Pour la plupart, ces enjeux font échos à certains thèmes précédemment évoqués. Ils ne concernent que les termes présents dans les

⁶²¹ Ce fait a été souligné plusieurs fois au cours des entretiens avec les gens travaillant dans l'administration française et également dans les entreprises.

⁶²² Pour les plus récents d'entre eux : LABORDES Pierre *La Sécurité des systèmes d'information - Un enjeu majeur pour la France*, Assemblée Nationale, 13 janvier 2006. ROMANY Roger, *Cyberdéfense, un nouvel enjeu de sécurité nationale*, Sénat, 8 juin 2008. BOCKEL Jean-Marie, *La cyberdéfense : un enjeu mondial, une priorité nationale*, Sénat, 18 juillet 2012

⁶²³ Il s'agit de la date des premiers documents officiels employant le langage étudié et l'idée de liberté des individus ou de données.

corpus analysés. Comme le démontrent les résultats, utiliser un terme composé du mot « cyber » revient pour une institution à parler de sécurité, et à rapporter cette sécurité à l’information comprise comme informatisée. Cette situation s’accroît dans le temps quel que soit le niveau de dialogue considéré. Cette thématique sécuritaire supplante totalement les autres thématiques considérées : libertés, accès à internet, gouvernement ouvert, transformation numérique de l’administration, enjeux des macro-données…

L’échelle retenue dans cette typologie classe les enjeux en trois catégories : principal, périphérique et marginalisé. Un enjeu principal est un enjeu « évident » dans sa consécration par le discours. Il sera doté d’un ou plusieurs mots composés du suffixe « cyber » et constituera souvent un domaine à part entière de compréhension de la sécurité de l’information. Les enjeux périphériques sont des enjeux qui pour s’exprimer ont besoin d’une démonstration afin de démontrer leur intérêt dans le discours.

Les enjeux marginalisés sont pour le moment exclus des thématiques portées par le discours. Ils n’en demeurent pas moins des enjeux importants de l’information qui peuvent être portés par d’autres discours et d’autres concepts que le cyberspace et ses variations. Ces derniers enjeux seront l’occasion d’aborder ces autres discours parmi les éléments de nuance⁶²⁴.

Il ne s’agira pas de détailler l’ensemble de ces enjeux mais de présenter sommairement leur positionnement thématique et leur articulation dans les corpus analysés.

1 – Enjeux principaux : menace, protection, sécurité, criminalité, défense.

L’idée de menace recouvre le potentiel d’une utilisation malveillante de l’informatique et sert de support à l’ensemble du discours au point d’y être érigée en postulat ontologique. Le discours opère ainsi le plus souvent un renversement de la dialectique classique d’une menace. En effet, le menace s’entend généralement de l’existence d’une faille de sécurité et de l’intention ou du moins de la possibilité de son exploitation par autrui. Ici, la menace repose le fait que le discours suppose l’existence permanente d’une fragilité inconnue quelconque et l’existence permanente d’une personne négligente ou malveillante pour transformer cette fragilité en vulnérabilité. De plus, la menace est subtile dans la mesure où voir sur le moment

⁶²⁴ Cf. infra, [...] Section III, E, 5.

que l'on est attaqué par l'informatique relève de moyens et de compétences qui ne sont pas nécessairement à la disposition de l'acteur. Les menaces mettent ainsi plusieurs années à être découvertes⁶²⁵. D'un autre côté, de nouvelles vulnérabilités sont découvertes quotidiennement et nourrissent une actualité chargée. En tant qu'objet du discours, la menace est un fait social total⁶²⁶. Autrement dit, la menace de l'information met en branle l'ensemble des composantes et des institutions de la société : elle peut être étendue à l'ensemble des secteurs. S'il est vrai que le « risque zéro » n'existe pas, c'est encore plus vrai en matière de cybersécurité. La sécurité informatique totale est un rêve. Les raisons sont nombreuses ; les failles dans les systèmes en sont une⁶²⁷. Concevoir et développer un système parfaitement sécurisé équivaudrait selon les chiffres de 2013 à une dépense 200 milliards d'euros⁶²⁸. Une somme qu'aucun acteur ne peut débourser. En effet, le marché global des technologies de sécurité informatique était de 14,8 milliards d'euros en 2013. Il est également bon de rappeler qu'une sécurité « totale » n'est pas techniquement souhaitable à moins de vouloir disposer d'une machine qui ne s'allume pas. L'informatique c'est comme une pièce dotée de nombreuses portes. Si vous fermez toutes les portes, l'utilisateur légitime ne peut plus employer votre système qui devient inexploitable.

D'un point de vue discursif, si la menace présente dans tout secteur informatisé, la criminalité représente la principale nature de cette menace. Son objet concerne principalement les entreprises, les flux financiers et le soutien à la criminalité classique. De manière paradoxale, les particuliers peuvent être touchés mais demeurent un élément secondaire dans le discours (quand bien même les données personnelles représentent l'un des plus grands enjeux de l'information depuis le début de la numérisation y compris dans la relation de ces particuliers avec l'administration). Toutefois, malgré son importance statistique la criminalité n'est que le premier terrain d'expression d'une menace perçue comme plus vaste. A partir du discours de la presse, nous pouvons établir une typologie des comportements d'agressions que peut

⁶²⁵ Par exemple, en mars 2014 les sociétés Google et Codenomicon ont identifié la vulnérabilité *Heartbleed* dans la bibliothèque de cryptographie *OpenSSL*. Cette vulnérabilité existait depuis mars 2012. Elle pouvait affecter certains téléphones et périphériques, ainsi que par exemple les sites Wikimédia, Soundcloud, Reddit, Tumblr, Prezi, Pinterest ou encore Sourceforge...

⁶²⁶ MAUSS Marcel, « Essai sur le don. Forme et raison de l'échange dans les sociétés archaïques », *l'année sociologique*, seconde série, 1923-1924, tome 1.

⁶²⁷ Le marché des failles inconnues et des codes permettant de les exploiter (« *0-day exploit* ») produit environ 85 failles inconnues par jour, une faille Windows inédite pourrait ainsi se vendre jusqu'à 250.000 dollars, voir notamment l'étude : PAGANINI Pierluigi, « Zero-Day Exploits in the Dark », *Infosec Institute*, 21 avril 2015. <http://resources.infosecinstitute.com/zero-day-exploits-in-the-dark/> [consulté le 1er août 2016].

⁶²⁸ Chiffres issus de la conférence du 28 mai 2013 à L'Ecole militaire (Paris) de Nicolas Ruff, alors chercheur en sécurité informatique au sein de la société Cassidian Cybersécurité.

potentiellement subir un individu à travers l'informatique : apologie de crime, arnaque, attaque, atteinte au secret de la correspondance, chantage, contrefaçon, crime, délit, dépendance, diffamation, diffusion d'images contre sa volonté, drogue, entrave, escroquerie, fraude, harcèlement, incitations diverses, injure, intrusion, malveillance, menace, pédophilie, piratage, prostitution, provocation raciste, racket, risque, sabotage, collecte ou traitement de données à caractère personnel illicite, virus, vol etc. Il existerait ainsi cinq grandes manières d'être victime de l'information : une atteinte aux biens (argent, données), une atteinte à la réputation, une exposition à des contenus violents et/ou illicites, la compromission de son système d'information ou l'exposition à la criminalité ordinaire⁶²⁹.

La protection représente l'ensemble des moyens pour parvenir à une sécurité face à cette menace. Ces moyens peuvent être de tout nature : politique, juridique, technique, physique... Toutefois, la protection en matière d'information se limite souvent à une composante de la sécurité comprise la sécurité des systèmes. Le discours « cyber » contient deux conceptions différentes de la sécurité : la sécurité des systèmes d'information et la cybersécurité. La sécurité des systèmes d'information vise à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées tel que prévu. Un système d'information sécurisée selon ce paradigme doit être intégral (non altéré dans son contenu), confidentiel (limitée aux personnes autorisées), disponible (accessible et dépourvu de failles de fonctionnement), non répudiable (ou traçable, l'ensemble des modifications est attribué au bon utilisateur) et faire l'objet d'une authentification (les utilisateurs sont identifiés par le système). A la différence du premier concept, la cybersécurité ne s'inscrit pas dans le but de protéger les systèmes d'information, mais fait de celle-ci un objectif nécessaire à la protection des utilisateurs (personnes ou organisations). Là où la sécurité des systèmes d'information est un objectif technique à court/moyen terme, la cybersécurité s'inscrit davantage dans un temps long et une vision globale qui comprend principalement des aspects politiques, économiques et humains relatifs à l'utilisation de ces systèmes. La conception française de la cybersécurité n'adopte

⁶²⁹ Il s'agit bien sûr d'une représentation schématique des types d'atteintes que peut subir le lecteur. En 2015, le ministère de la justice français relevait, dans la base de données NATINF, 248 infractions (crimes, délits et contraventions de 5ème classe) pour lesquelles l'objet ou le moyen utilisé relève, selon le texte légal d'incrimination, de la cybercriminalité. A ces premières infractions, se rajoutaient également 181 infractions supplémentaires pour lesquelles le texte d'incrimination ne fait pas référence à la cybercriminalité mais dont la commission au moyen d'un système d'information est avérée, ainsi que 46 infractions prévues par le code des postes et des communications électroniques, qui paraissent aussi relever de la cybercriminalité. Voir notamment, les données du groupe de travail interministériel sur la cybercriminalité.

toutefois pas cette approche holiste et demeure marquée par une vision technocentréة. Ainsi pour l'Agence nationale pour la sécurité des systèmes d'information (ANSSI), la cybersécurité est un « état recherché » pour un système d'information lui permettant de résister à des événements « issus du cyberespace » susceptibles de compromettre « la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles⁶³⁰. L'idée est que « la cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense ».

Dans ce contexte, la défense qui a déjà été abordée auparavant apparaît comme un thème secondaire du discours. Elle n'est portée principalement que par le corpus 1, où elle n'arrive pas en tête des préoccupations premières. Toutefois, la thématique de la défense possède une importance influence sur l'ensemble du discours analysé. En effet, si la défense et plus spécifiquement ses aspects militaires concernent finalement un secteur d'application de la sécurité. Les principes, les normes et les processus définis dans ce secteur vont servir de modèles pour la sécurité de l'information en général (y compris lorsque sont exclus les cas où des liens organiques existent entre la cybersécurité et des composantes militaires ou du renseignement des États en question). Cette influence prend la forme particulière d'une culture de l'information.

2 – Enjeux périphériques : gouvernance, gestion des flux de données, résilience.

La thématique de la gouvernance n'apparaît pas ici nécessairement parmi les enjeux principaux du fait que le discours insiste sur la place de l'acteur régional⁶³¹. De plus, cette thématique existe de manière autonome sur l'idée de gouvernance d'Internet. D'après les résultats, la gouvernance du cyberespace (ou cybergouvernance) ne suscite qu'assez peu d'intérêt en elle-même. Toutefois, le principe même de la gouvernance, soit l'élaboration commune et l'application de principes régulateurs par les États, les organisations internationales et la société civile, semble être le modèle applicable aux enjeux politiques les plus importants comme par exemple : la cybercriminalité⁶³². L'enjeu de la gouvernance est

⁶³⁰ ANSSI, *Défense et sécurité des systèmes d'information, Stratégie de la France*, 2012, p. 21.

⁶³¹ En revanche, sortie du discours cyber elle sera l'un des thèmes politiques les plus importants du côté de la recherche.

⁶³² DUPONT Benoît, 2016, op-cit.

donc plus vaste que le seul objet Internet dont gouvernance se limite aux questions des noms de domaines, des adresses IP, des langues, ainsi que de l'accès à Internet et de la consommation en énergie de ce dernier (comme aspect de l'impact environnemental). La gouvernance d'Internet se distingue ici de la cybergouvernance par une spécificité d'objet. Il est possible de distinguer ces deux ensembles de l'administration électronique et la propriété intellectuelle numérique qui sont deux autres ensembles. Le premier intéresse principalement la manière dont les administrations utilisent l'informatique dans leur fonctionnement normal. La seconde s'intéresse à la propriété des contenus numériques. Ce partage vient renforcer l'aspect sécuritaire de la cybergouvernance (Même si ces domaines ne se conçoivent pas nécessairement de manière exclusive). Le rôle de la gouvernance dans le discours consiste en l'énonciation d'un objectif de coopération autour de la définition de norme commune entre les États avec les autres organisations.

La gestion des flux de données est une thématique complexe qui recoupe plusieurs problèmes liés à l'infrastructure du réseau. L'idée générale est celle de la nécessité de gérer les échanges d'information d'un point de vue physique et logique. Cette gestion appelle plusieurs catégories de questionnements que l'on retrouve pour beaucoup d'entre elles dans le corpus 3 mais il est possible de les retrouver dans les corpus 4 et 5. Premièrement, la soutenabilité de la croissance du réseau pose question. Le réseau des réseaux pourra-t'il croître suffisamment vite dans l'ensemble de ses composantes pour soutenir une croissance de capacité ? Et à quelles conditions (techniques, juridiques, énergétiques) ? Du point de vue des entreprises, la question semble se poser notamment chez les opérateurs de téléphonie et dans le secteur bancaire. Deuxièmement, le réseau est-il suffisamment robuste et résilient pour pouvoir être maintenu en cas de défaillance ? La question d'une défaillance généralisée des systèmes d'information représente actuellement l'un des scénarios les plus grave (et les moins probables) en termes de menace. Toutefois, l'histoire (et les corpus) regorgent d'exemples qui mettent en avant la fragilité de telle ou telle partie du réseau. Par exemple, le 28 mars 2011, Internet a été coupé dans l'ensemble du territoire arménien par suite d'un coup de bêche donné par une femme de 75 ans sur un câble de fibre optique reliant l'Arménie à la Géorgie, ce alors qu'elle cherchait à récolter du cuivre pour le revendre⁶³³. Dans un troisième temps, se pose la question du parcours

⁶³³ La nouvelle a d'abord été médiatisée par le journal britannique The Guardian avant d'être reprise par les journaux francophones. PARFITT Tom, « Georgian woman cuts off web access to whole of Armenia », *The Guardian*, 6 avril 2011.

de l'information dans le réseau et la gouvernance d'Internet à ce sujet. C'est toute la question du *peering* (l'échange de trafic Internet) au travers point d'échange Internet⁶³⁴. Ce dernier point assez technique est peu présent dans le discours analysé.

Enfin, la résilience désigne une aptitude pour un système de retrouver ses propriétés initiales après une altération. Cette altération, quel que soit le secteur où l'idée de résilience est employée, est subie par l'acteur qui doit avoir une réaction. Le système de référence qui peut être un système technique ou une organisation humaine est capable de s'adapter à des conditions changeantes, de résister et de récupérer rapidement à la suite de perturbations subies. La cyberrésilience correspond à une thématique émergente en matière de sécurité de l'information. Un intérêt de résilience sur le terrain de l'information pour l'acteur ne permet pas seulement de garantir la continuité de son existence, il répond également d'une forme de « vouloir être ». Une cybersécurité fiable et absolue est difficile à mettre en place. Elle est impossible car elle ne peut être garantie sans y mettre un prix colossal⁶³⁵. Si on admet que cette mise en place relève du domaine du possible, elle signifie la fin de l'utilisabilité du système. Fort de cet apport, la cybersécurité suppose en pratique la détermination d'un « sacrifice acceptable ». Ce sacrifice sera acceptable à partir du moment où même si celui-ci devient effectif, l'organisation pourra continuer ses activités dans les conditions prévues. La résilience est en tant que concept est la limite à partir de laquelle un modèle de sécurité peut accepter une part d'insécurité. La résilience détermine donc un seuil de menace acceptable.

⁶³⁴ Voir notamment parmi les travaux récents : DENARDIS Laura, « Governance at the Internet's Core: The Geopolitics of Interconnection and Internet Exchange Points (IXPs) in Emerging Markets », Conférence 2012 TRPC Research Conference on Communications, Information and Internet Policy, 22 mars 2017.

⁶³⁵ Cf. Supra.

Conclusions de chapitre.

Le contexte d'emploi des termes dérivés du cyberespace qu'à mis en avant l'étude réalisée dans ce chapitre met en avant une association du cyberespace avec des enjeux politiques différents au sein desquels la thématique générale de la sécurité est dominante. Les corpus mettent en avant une variation dans les topiques qui décrit un horizon des priorités qui change en fonction de l'acteur et en fonction du temps. En matière de normes, de langage et de priorités, le cyberespace n'a donc rien d'universel.

D'après les éléments de discussions qui ont été relevé, il y a des enjeux principaux du discours : menace, protection, sécurité, criminalité, défense. Lesquels sont rejoints par quelques thématiques secondaires : gouvernance, gestion des flux de données, résilience. Des thématiques secondaires existent et touchent principalement à l'accès à Internet (Corpus 3 et 4) et à la défense des libertés (Corpus 2 et 3). Bien que cette dernière puisse également être associée à la sécurité par l'individu

Parmi les enjeux, la thématique « défense » pourrait apparaître comme un sujet secondaire par rapport à la sécurité et à la criminalité si elle n'était pas au cœur des préoccupations de l'État. Notons encore une fois que ce dernier semble quantitativement avoir un cran de retard par rapport à l'ONU et l'UE. Cela pourrait être une piste concernant une influence internationale. Toutefois, cette hypothèse ne nous semble pas nécessairement pertinente à la lumière de ces seuls résultats.

Au niveau local, l'échelon régional efface complètement la dimension internationale (corpus 4 et 5) mais des thématiques communes se retrouvent notamment dans les libertés et la résilience.

L'ensemble analysé renvoie vers deux acteurs clefs : l'État et l'individu qui semblent opposés sur la question des enjeux. Les discours analysés mettent par ailleurs en avant une position clef de l'acteur régional ; là où l'individu semble apparaître à la marge dans les niveaux locaux et internationaux. Il est encore trop tôt pour conclure à une opposition entre sécurité individuelle et nationale (D'autant que nous n'analysons qu'un seul corpus étatique). Toutefois, il est possible d'affirmer que par les thématiques et la manière dont elles sont traitées l'acteur régional apparaît comme dominant. La coopération internationale semble être un enjeu limité

voire marginaliser. C'est là une énorme différence entre les discours et les pratiques internationales que nous aurons l'occasion de démontrer avec plusieurs exemples par la suite.

En effet, à la lecture de ces données, le cyberespace et les termes dérivés ne semblent pas incarner un enjeu international fort. Certes les différents corpus contiennent des résultats (particulièrement le corpus 2). Toutefois, à l'échelle de l'importante période de temps analysé les résultats demeurent assez réduits d'un point de vue quantitatif.

Le contexte d'emploi du langage « cyber » varie également dans le temps. Le nombre de résultats augmentent avec les années dans chaque corpus. Les résultats obtenus permettent de fixer un point de bascule général dans l'année 2008. Ce qui correspond aux récits classiques sur la thématique « cyber » évoqués en introduction. Le pic d'influence semble ici être autour des années 2013 à 2015 en fonction des corpus. Les résultats ne nous permettent pas d'en déduire les causes. Des analyses plus avancées sont nécessaires.

Combiné avec les résultats du premier chapitre, nous pouvons en déduire que le langage « cyber » a été consacré comme étant associé à la sécurité durant l'année 2008. Cela voudrait dire que la transformation de l'enjeu de l'information à l'aide de l'opérateur de conversion du langage a eu lieu entre 2001 et 2008 avec probablement une accélération autour de 2008.

Afin d'avancer davantage dans l'analyse du discours, nous allons quitter le domaine du quantitatif pour nous intéresser au qualitatif en nous intéressant au terrain de cette recherche à travers le concept de communauté épistémique.

Chapitre 3 – Le phénomène linguistique « cyber » : la communauté épistémique comme communauté discursive.

« La connaissance scientifique est la colle qui permet aux acteurs politiques de rester engagés et peut être utilisée comme une carte maitresse contre les opposants à la coalition épistémique. »

Clair GOUGH et Simon SHACKLEY⁶³⁶

De cette recherche visant à comprendre comment le cyberespace pouvait influencer les Relations Internationales, a rapidement émergé le besoin de comprendre ce à quoi le terme renvoyait du point de vue de la recherche académique. Seulement, cela a entraîné deux difficultés particulières. La première difficulté rencontrée est que le phénomène linguistique relatif au cyberespace n'est pas limité à un public universitaire mais implique la participation de nombreux acteurs. Dès lors, le sens de ce phénomène dépasse les limites de son caractère « scientifique ». Travailler sur le cyberespace dans la recherche française amène inévitablement à rencontrer les acteurs d'une communauté bien plus vaste : celle de l'ensemble des locuteurs de ces discours. Deuxièmement, cette communauté discursive fait de la recherche un enjeu important de médiation et de légitimation des acteurs participants au débat. Les frontières de la communauté discursive ne sont plus simplement « scientifique » mais résultent d'autres relations entre les membres de celles-ci. Pour aborder le phénomène « cyber » sous l'angle communautaire et conceptuel, il faut donc se pencher sur la covariation du discours et des saillances épistémiques de la communauté des locuteurs de ce même discours.

S'interroger sur le caractère épistémique de ce phénomène communautaire revient à rechercher la capacité de tout ou partie de la communauté discursive à influencer le politique. Cette compréhension spécifique de la communauté épistémique passe par une relecture du concept à l'aune d'une combinaison de l'épistémologie de Jean-Claude Passeron avec les apports précités de Mai'a Davis Cross ainsi que de William J. Drake et Kalypso Nicolaïdis. Dès lors, la communauté épistémique pourra être comprise un espace dynamique de redistribution

⁶³⁶ GOUGH Clair et SHACKLEY Simon. « The respectable politics of climate change: The epistemic communities and NGOs » *International Affairs*, Vol. 77, No. 2, avril 2001, pp. 329-345. (Notre traduction).

des rapports de force dans l'espace sémantique entre plusieurs discours autour d'un même enjeu, qui peuvent influencer ce que Passeron désignent comme les « compréhensions du monde historique » et avoir un impact sur de vastes ensemble de normes.

S'inscrivant dans la lignée des chapitres précédents, ce chapitre a ainsi pour but d'opérer un mélange entre la communauté épistémique et l'analyse de discours à partir du point de vue Français. Ce chapitre interroge ainsi à la fois le cadre théorique de la thèse et son terrain. De cette manière, le présent chapitre formera les prémisses d'une synthèse du phénomène observé entre les éléments historiques, logométriques et le terrain de cette recherche.

La relecture de la communauté épistémique sous le prisme du discours sera l'objet une première section. La deuxième section de ce chapitre sera consacrée à la mise en avant des traits communs du discours objet de production de la communauté par la définition de ses frontières. La troisième et dernière section sera dédiée à la construction de la communauté « cyber » en France à travers de l'influence américaine, de l'émergence de la sécurité de l'information et de sa transformation en enjeu de sécurité. Cette troisième section terminera par le terrain de recherche.

Section 1 – De l'émergence de la production d'une communauté épistémique dans le champ sémantique.

La communauté épistémique se conçoit comme un réseau d'experts qui persuadent autrui avec leurs normes communes et leurs objectifs politiques en vertu de leurs connaissances professionnelles. C'est la principale contrainte de la notion de communauté épistémique : tous ses membres doivent avoir l'expertise nécessaire pour comprendre les problèmes, interpréter les informations, pour définir des objectifs de manière commune. Toutefois, cela ne suffit pas vraiment à caractériser l'existence d'une communauté épistémique. En effet, une telle communauté sera ou ne sera pas une communauté épistémique.

Encore faut-il que la communauté partage le même jugement professionnel sur un enjeu particulier, puisse évaluer la validité de ses objectifs politiques dans son ou ses domaines de compétence, opte pour un ensemble commun de pratiques en ce qui concerne l'enjeu en

question et partage des principes, des croyances, des valeurs⁶³⁷. Ces critères sont compris, d'après Mai'a Davis Cross⁶³⁸, sous l'angle de la professionnalisation et du professionnalisme comme sédiment de la cohésion communautaire.

De plus, la communauté n'existe pas simplement, elle peut être forte ou faible selon la variation de son pouvoir d'influence. Le travail des communautés épistémiques est continu et n'a pas besoin d'une crise pour exister. Et enfin, une communauté épistémique peut inclure d'autre type de connaissances que la connaissance scientifique. Confronté à une communauté d'expert la question demeure de savoir reconnaître la nature épistémique de celle-ci ou de pouvoirs l'exclure.

Cette section reviendra donc sur l'emploi de la communauté épistémique : les différents critères pour reconnaître sa présence, déterminer sa capacité d'influence et sur la manière de l'articuler avec notre approche du discours au travers d'une compréhension discursive de l'influence et des phénomènes de concurrence entre les différents discours au sein de la communauté épistémique.

A – Critère de présence de la communauté épistémique : de l'intégration à la production.

Pour pouvoir analyser une communauté épistémique encore faut-il qu'il y ait un phénomène communautaire. Les trois indicateurs de l'existence d'une communauté épistémique reposent principalement sur le décloisonnement des cadres bureaucratique au profit des échanges et de la construction d'une culture professionnelle commune⁶³⁹. Même si de nombreux obstacles peuvent limiter l'émergence d'une communauté épistémique.

Le premier indicateur repose sur une forme d'holisme qui veut que pour une communauté épistémique, le tout formé soit plus grand que la somme des parties. Autrement dit lorsque la communauté d'experts dépasse les assignations bureaucratiques traditionnelles de

⁶³⁷ HAAS Peter M., 1992 op_cit. p.3. L'auteur conserve ces critères par la suite voir notamment : HAAS Peter M. (2001). « Policy knowledge: epistemic communities ». In SMELSER Neil J. et BALTES Paul B. (eds.), *International Encyclopedia of the Social and Behavioral Sciences*, Elsevier, 2001. pp. 11517 - 11578.

⁶³⁸ Cf. Chapitre liminaire. CROSS Mai'a K. Davis. 2012, pp. 137–160.

⁶³⁹ CROSS Mai'a Davis, The Limits of Epistemic Communities: EU Security Agencies », Politics and Governance, vol 3, n°1, 2015 pp. 90-100.

chacun de ses membres et va aller au-delà des simples attentes formelles en tant que groupe. Cela implique notamment une forme de persuasion autour du caractère nouveaux des initiatives du groupe et leur précédente inexistence ou insuffisance. Des obstacles à cet indicateur existent lorsqu'un groupe garde une trop forte adhésion à sa mission originelle ou lorsque le cadre des échanges favorise un environnement professionnel contraint formel et restrictif. Un deuxième indicateur est celui de l'antériorité de la relation professionnelle matérialisé par des rencontres précédentes entre les membres de la communauté. Ceux-ci peuvent avoir travaillé ensemble dans des travaux antérieurs, en ayant les mêmes positions à plusieurs reprises ou de manière successive, ou ils peuvent tout simplement être en interaction informelle en dehors du travail... Ce deuxième indicateur vise à découvrir l'existence de buts professionnels communs, voir le développement de ce que Mai'a Davis Cross nomme un « esprit de corps »⁶⁴⁰. Nous pourrions assimiler ce dernier à un sentiment d'appartenance partagé. Ce dernier peut ne pas exister lorsque la communauté est formée de membres qui n'ont jamais travaillé ensemble ou cultivent un réseau d'interactions trop vastes qui minent l'apparition d'objectifs commun. Un troisième et dernier indicateur implique que les membres de la communauté épistémique partagent des normes professionnelles et une culture distincte de leur « bureaucratie » originelle. Cela se vérifie par des rencontres fréquentes, de haute qualité, efficaces au sens où le temps est majoritairement consacré aux questions de fond. Il en résulte des accords et des positions communes qui dépassent normalement le plus petit dénominateur commun. L'obstacle principal est qu'une culture professionnelle est souvent liée à une institution. Un autre obstacle est une limitation au caractère procédural des normes sans pouvoir le dépasser.

Il en ressort qu'un groupe organisé autour de fonctions hiérarchiques strictes et formelles ne peut pas favoriser l'émergence d'une communauté épistémique sans remettre tout ou partie de cette organisation en question. Une communauté épistémique implique une forme d'horizontalité et de masse critique qui favorise son émergence. Un tel groupe d'experts favorisera son mandat originel sans dépasser les limites de l'autonomie qui lui est accordé. Dès lors, cela réduira son pouvoir d'influence et en fera une communauté faible. De la même manière, les professions qui ont une culture du secret dominante sur le partage (comme cela est le cas dans la sécurité de l'information) limitent également l'émergence d'une communauté épistémique.

⁶⁴⁰ En français dans le texte, Ibid, p. 92.

1 – De la connaissance scientifique à la connaissance experte.

La rupture avec l’impératif de la connaissance scientifique et de sa valorisation (à travers les publications et du mécanisme de revue en double aveugle) représente sans doute l’une des grandes différentes avec les approches des années 90. Est-ce qu’un expert peut être autre chose qu’un scientifique ? Mai'a Davis Cross prend l’exemple des membres haut-gradés de la profession militaire qui possèderaient une connaissance spécialisée des opérations militaires et de leur conduite, capable de couvrir l’orientation des forces, la stratégie, ou encore la logistique. Elle ajoute que l’expertise militaire partagée a évolué en Europe au point de faire exister des phénomènes transnationaux de transfert d’expertise par le biais des alliances, comme par la concurrence des systèmes de forces dont l’exemple le plus parlant demeure l’émergence dans l’enseignement des écoles militaires pour la formation des officiers qui suivent pour la plupart des schémas type de l’enseignement supérieur civil caractérisé par une forte ambition en terme de formation et l’ouverture à l’international⁶⁴¹. Elle prend notamment l’exemple de l’académie militaire de Westpoint, du l’académie militaire de l’état-major général de Moscou et des Ecoles de Saint-Cyr en France. Elle ne suggère pas que toute la profession militaire puisse constituer une communauté épistémique (on parlerait alors de communauté de pratiques), mais que certains officiers haut-gradés de l’armée puissent former des communautés épistémiques à travers leurs échanges transnationaux du fait d’une culture professionnelle partagée. La question de l’influence de la politique demeure.

L’auteure met en avant le rôle actif des officiers généraux membres permanents du comité militaire de l’Union Européenne lors de la conception d’*Une première vision à long terme pour les capacités et besoins en capacités de l’Europe en matière de défense*⁶⁴². Un autre exemple de communauté épistémique cité par l’auteur est celle formée par les diplomates⁶⁴³. Les deux raisons pour refuser de reconnaître les groupes de diplomates comme une communauté épistémique sont d’une part le profil « généraliste » (et non pas « expert) des diplomates, et d’autres part le fait qu’ils représentent directement les intérêts des États. Même

⁶⁴¹ CROSS Mai'a K.Davis, 2012, Op-cit. p. 157-158

⁶⁴² CROSS Mai'a K. Davis, *Security IngrÉtation in Europe, How Knowledge-Based Networks Are Transforming the European Union*. Ann Arbor: University of Michigan Press, 2011. pp. 177 – 185.

⁶⁴³ CROSS Mai'a K. Davis, *The European Diplomatic Corps: Diplomats and International Cooperation from Westphalia to Maastricht*, 2007, Londres, Palgrave Macmillan, 244 p.

si leur expertise en matière de négociation, leurs normes professionnelles partagées et leur capacité à transcender leur rôle par la formation de groupes de travail informels, peuvent leur permettre de constituer des communautés épistémiques⁶⁴⁴. Enfin, le troisième exemple sélectionné concerne la prêtrise et les leaders religieux qui mobilisent leur expertise herméneutique dans une communauté épistémique⁶⁴⁵.

2 – La connaissance face au paradoxe du professionnalisme communautaire

Dans cette formulation, la communauté épistémique nous semble faire face à une forme de paradoxe : l'exigence d'une culture professionnelle commune. Or si la communauté épistémique n'est pas une communauté de pratique, elle exigerait une forme de culture professionnelle commune de la part de personnes (qui ne partagent pas nécessairement dans les faits la même origine professionnelle). Autrement dit, une communauté épistémique est plus forte lorsqu'elle incarne un espace émergent dans lequel l'échange des connaissances peut s'effectuer en dehors des contraintes organisationnelles (donc une communauté de pratique⁶⁴⁶).

C'est ici qu'il faut insérer l'idée de la connaissance afin de dépersonnaliser la communauté et poser la question de la production de celle-ci en la différenciant de l'intégration communautaire. Le point de basculement pour l'émergence d'une communauté épistémique semble être le fait que les connaissances dont elle est experte deviennent une forme d'action politique⁶⁴⁷. Il ne suffit pas de « se focaliser sur ce qu'elles partagent et ce qui les tient ensemble, ni de voir ces communautés comme des entités stables et délimitées » : les communautés doivent être des « cibles mouvantes »⁶⁴⁸. Une communauté n'existe pas en un seul endroit. L'entité assimilable à une communauté y fait en réalité figure d'exception. La communauté existe avant tout par ses discours et les pratiques des experts (notamment scientifiques) qui visent à construire, à mettre en ordre, à faire évoluer leurs communautés jusqu'à transformer celle-ci en lieu de travail politique. Le professionnalisme d'une communauté ne se doit pas

⁶⁴⁴ Sur les groupes dans le cadre de la diplomatie, voir la troisième partie de l'ouvrage concernant les différents secteurs de la diplomatie : BALZACQ Thierry, CHARILLON Frédéric et RAMEL Frédéric, *Manuel de diplomatie*, Paris, Science Po, 2018, pp. 245 – 352.

⁶⁴⁵ SANDAL Nukhet.. « Religious actors as epistemic communities in conflict transformation: The cases of South Africa and Northern Ireland. » *Review of International Studies*, Vol. 37, 2011, pp. 929 – 949.

⁶⁴⁶ WENGER Etienne, 1999, op-cit.

⁶⁴⁷ AKRICH Madeleine, 2010, op-cit.

⁶⁴⁸ Deux citations issues de MEYER Morgan, et MOLYNEUX-HODGSON Susan, 2011, op-cit, p. 150.

s’apprécier à partir d’un paradigme culturel, mais doit partir de la production de la communauté. Dès lors, selon l’approche de Morgan Meyer et Susan Molyneux-Hodgson⁶⁴⁹, la communauté épistémique revêt quatre caractéristiques qui fondent son intérêt du point de vue de la connaissance. Toutefois, à l’opposé de cette approche, cette communauté ne s’inscrira pas nécessairement dans le monde scientifique.

Premièrement, les communautés épistémiques ont avant tout pour objet, média et finalité la connaissance. Elles « produisent, publicisent et politisent des connaissances »⁶⁵⁰. Une communauté doit être capable d’organiser hiérarchiquement la conception, l’organisation, la valorisation, la vérification, l’inventaire et le stockage de la connaissance. Autrement dit, la communauté se doit de disposer d’un discours cohérent qui rationnalise la création et l’emploi de son expertise. A l’échelle de la communauté, nous qualifierons ce travail de production. Ce travail particulier souscrit à notre premier indicateur qui veut que la production communautaire dépasse la somme de la production de ses membres (et de leurs « liens bureaucratiques traditionnels »). Le rapport de la communauté à la connaissance, donc à la production, restaure une forme d’horizontalité. Deuxièmement, l’existence de ces communautés obéit à un processus de fabrication et de stabilisation dont la finalité réside dans la communauté. La réalisation de la communauté et son identification sont des comportements parallèles sinon connexes à sa production. La communauté est ainsi produite par son propre discours, mais également avec des évènements et des dispositifs extérieurs à la communauté. Troisièmement, à l’inverse, une communauté doit être comprise comme dynamique. Si son travail de connaissance est permanent, elle peut être ou ne pas être un lieu de travail politique (ce qui rejoint l’idée d’influence politique communautaire). Ces transformations sont liées à des facteurs exogènes comme endogènes à la communauté. Enfin, au-delà d’objets de connaissance, une communauté épistémique se reconnaît en ce qu’elle produit des « producteurs de connaissances » : « elles façonnent, délimitent et articulent les identités de producteurs de connaissance actuels et futurs et elles façonnent des trajectoires individuelles et collectives le long desquelles ces derniers naviguent »⁶⁵¹. Ces derniers points se rapprochent de la notion de

⁶⁴⁹ Ibid, pp. 150 et 151.

⁶⁵⁰ Ibid. p. 150

⁶⁵¹ Ibid. p 151

professionnalisation de Mai'a Davis Cross et des deuxième et troisième indicateurs qui replacent la relation des membres de la communauté dans le temps long.

B – Critères d'influence d'une communauté épistémique.

Dans la perspective proposée en 2012 par Mai'a Cross⁶⁵², l'une des questions fondamentales est la détermination des conditions dans lesquelles une communauté épistémique compte. C'est le cas lorsque celle-ci dispose d'un pouvoir de persuasion. Autrement dit, le principal caractère d'une communauté épistémique réside dans son pouvoir d'influence à l'égard du politique.

La question est donc de savoir si la communauté identifiée souscrit aux différents critères de cette persuasion. Ceux-ci relèvent principalement de la cohérence interne de la communauté et de diverses conditions environnementales. Une communauté sera perçue comme plus persuasive en fonction du nombre de situations dans lesquelles elle peut s'inscrire. L'auteure construit sa lecture de l'influence des communautés épistémiques à partir des travaux d'Anthony Zito⁶⁵³ autour de cinq catégories de conditions d'influence : *Scope conditions, political opportunity structure, phase in policy process, coalition building, policy field coherence*. Dans notre étude nous regrouperons ces différentes conditions en trois types : les conditions relatives à l'enjeu, à la relation entre la communauté et l'environnement politique et enfin les conditions dépendantes de la cohérence de la communauté.

1 – Le principe d'incertitude comme condition fondamentale de l'influence communautaire.

La condition fondamentale qui permette l'influence de la communauté épistémique est l'incertitude continue concernant la crise perçue. L'ontologie de l'incertitude veuille qu'une décision politique suppose une incertitude réduite. L'incertitude est dite continue lorsqu'elle cumule un haut degré de visibilité avec un haut degré d'incertitude de l'enjeu. C'est alors

⁶⁵² CROSS Mai'a K, 2012, Op-cit. p. 142-144.

⁶⁵³ ZITO Anthony R. « Epistemic communities, collective entrepreneurship and European integration », Journal of European Public Policy, vol 8, n°4, 2001, pp. 585-603

qu'elle peut permettre l'influence de la communauté épistémique⁶⁵⁴. Le fait que l'incertitude puisse être reliée à l'enjeu dépend d'un contexte de crise perçue. D'une part, il y a une crise perçue lorsque l'incertitude résulte d'un enjeu complexe et/ou nouveau qui appelle l'intervention de l'expertise⁶⁵⁵. D'autre part, lorsque les décideurs cibles de la communauté ne sont pas satisfaits de l'adéquation des anciennes politiques face à aux problèmes liés à l'enjeu en question⁶⁵⁶. L'incertitude existe partout et ne se limite pas à une compréhension des circonstances des faits ayant entraînés une crise majeure. Il faut insister sur l'importance de la perception de l'incertitude : même si un enjeu est a priori objectivement certain, il peut être perçu comme incertain⁶⁵⁷. L'ontologie de l'incertitude favorise ainsi une compréhension structuraliste de la communauté épistémique qui existe toujours (de manière plurale et dynamique) et est toujours au travail (présence continue peu importe l'enjeu).

Concernant la communauté objet de notre analyse, cette incertitude de l'enjeu de la sécurité de l'information tire sa force de la complexité accrue du fait de la diffusion des systèmes d'information regardée comme nouvelle et croissante ainsi que des progrès techniques réalisés en matière d'informatique (dont de nombreux secteurs sont aujourd'hui dépendants). En effet, l'informatique n'est pas un secteur ordinaire. Au-delà de sa seule diffusion, l'informatique supplante sa propre compétence à celles d'autres domaines d'expertise sur des secteurs qu'elle alimente. Cette complexité nouvelle du fait de la grande disponibilité et de la dépendance liées à l'artefact et de ses effets entraîne une forme d'inadéquation perçue du cadre normatif chargé de l'appréhender. Par ailleurs, cet outil se voit également attribué une capacité de contourner sinon violer un certain nombre de règles.

Dès lors l'incertitude amène à questionner les règles mises en place pour savoir si elles sont toujours adaptées et/ou applicables à cet enjeu. L'incertitude concerne non-seulement le

⁶⁵⁴ Cette perspective est issue des travaux sur la technocratie de Claudio Radaelli. Lorsque l'incertitude est basse et l'enjeu visible, la décision politique sera dominante. Lorsque l'enjeu est peu visible, le modèle montrera l'influence des politiques bureaucratique (incertitude basse) et technocratique (incertitude haute). RADAELLI Claudio M., (1998), *Technocracy in the European Union*, Londres, Routledge, 2017, 184 p.

⁶⁵⁵ RADAELLI, Ibid. Voir également sur les implications des problèmes environnementaux dans le premier chapitre consacré à la pollution de l'ouvrage HAAS Peter M. *Saving the Mediterranean: The Politics of International Environmental Cooperation*, Columbia University Press, 1990, pp 17 – 25.

⁶⁵⁶ HALL Peter A. « Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain », *Comparative Politics*, vol. 25, no. 3, 1993, pp. 275–296.

⁶⁵⁷ Voir l'exemple du changement climatique. CROSS Mai'a K, 2012, Op-cit. p. 152.

régime des politiques publiques, mais également les décisions, la nature des normes et les modèles de représentations du monde qui les portent. Si l'incertitude crée un espace dans lequel la communauté épistémique peut porter une activité⁶⁵⁸, elle n'explique pas totalement l'impact de cette activité.

2 – Une influence politique déterminée par des conditions structurelles et processuelles.

La question de la détermination de l'influence sur le politique est au cœur des travaux sur les communautés épistémiques (comme de leurs critiques). Elle suppose l'accès à tous les décideurs nécessaires, ainsi que l'anticipation de leurs besoins et de leurs actions⁶⁵⁹. Cette influence se positionne en amont des politiques publiques dans les termes du débat initial plutôt que dans la décision, et plutôt dans la couche administrative/technocratique que dans les frontières des croyances politiques⁶⁶⁰. Dans le cadre d'une critique du concept, cette persuasion peut exister, mais elle serait du domaine de l'exception plutôt qu'une tendance forte des Relations Internationales. Les communautés épistémiques pourraient dominer la décision gouvernementale sur des questions apparemment techniques mais seraient surestimées.

« [...] En ce qui concerne la pollution ou les détails de l'emploi des forces militaires, le mécanisme semble moins bien décrire la manière dont les chefs d'État acquièrent leurs informations sur des questions fondamentales relatives aux relations internationales. »⁶⁶¹

Cette critique de Ronald Krebs met en avant une distinction fondamentale au sein de la capacité d'influence d'une communauté entre la manière dont le décideur acquière les détails techniques sur un enjeu particulier qui peut être le rôle d'une communauté épistémique et les

⁶⁵⁸ Voir le concept d'« émergence ». ADLER Emanuel. « The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control. » *International Organization*, vol. 46, no. 1, 1992, pp. 101–145

⁶⁵⁹ Sur l'accès : HAAS Peter M., 1992, op-cit. ainsi que DRAKE William J., et NICOLAIDIS Kalypso, 1992, op-cit. Sur l'anticipation des besoins futurs: RICHARDSON Jeremy, « Actor Based Models of National and EU Policy-Making: Policy Networks, Epistemic Communities and Advocacy Coalitions » In HUSSEIN Kassim et ANAND Menon (eds), *The EU and National Industrial Policy*, London: Routledge, 1996, pp. 26–51.

⁶⁶⁰ Sur les termes initiaux du débat et la présence dans la couche administrative : PETERSON John et BOMBERG Elizabeth, *Decision-Making in the European Union*, Londres, Macmillan International, 1999, 352 p.

⁶⁶¹ Notre traduction. KREBS Ronald R, « The Limits of Alliance: Conflict, Cooperation, and Collective Identity: Essays on International Relations in Honor of Rich ». In. LAKE Anthony & OCHMANEK David (eds), *The Real and the Ideal: Essays on International Relations in Honor of Rich*. Rowman and Littlefield/Council on Foreign Relation, Lanham, Maryland, 2001 p. 225.

enjeux politiques proprement dit pour lesquels un décideur ne ferait pas appel à une communauté épistémique. Cette critique semble un peu mal fondée dans sa division car elle s'inscrit en faux par au rôle traditionnel de l'expertise y compris sur les « questions fondamentales » des Relations Internationales... Néanmoins, elle permet d'étendre la compréhension de la communauté épistémique au-delà des seuls scientifiques pour y inclure d'autres acteurs. Par ailleurs, elle interroge le rôle du gouvernement dans la constitution des communautés épistémiques.

Pour comprendre la nature de l'influence des communautés William Drake et Kalypso Nicolaïdis distinguent trois niveaux : environnemental, politique et conceptuel⁶⁶². Le niveau « environnemental » produit l'identification initiale des nouveaux enjeux. Le niveau politique intervient pour deux fonctions particulières que sont les « intérêts nationaux » (Institutions, capacités de compétition, relations État-société, idéologies) et le « cadre de négociation » qui effectue la redistribution des intérêts et des positions sur des enjeux spécifiques afin de parvenir à un résultat qui correspond à la décision. Ce niveau politique échange avec le niveau conceptuel (communauté épistémique) soit en ce qu'il lui demande des idées nouvelles, soit à travers les canaux d'influence réciproque lorsque la communauté intervient dans le cadre de négociation. Dès lors la communauté épistémique peut avoir deux types d'impacts : définir les enjeux, spécifier des options de politiques pour traiter les enjeux en question.

Mai'a Davis Cross souligne qu'il existe de nombreuses possibilités entre les communautés qui travaillent avec les gouvernements dans des programmes communs, les communautés hébergées au sein des gouvernements...⁶⁶³ Elle introduit alors l'idée de professionnalisation communautaire dont la fonction première est de sortir la communauté du confinement imposé par les liens formels ou bureaucratiques de ses membres ; et dont la seconde fonction sera de délier le concept d'une communauté épistémique d'une communauté scientifique.

⁶⁶² DRAKE William J., et NICOLAIDIS Kalypso, 1992, op-cit. p. 42

⁶⁶³ CROSS Mai'a K Davis, 2012, Op-cit. p. 154-155.

3 – Une influence alimentée par la cohérence de la communauté.

Le degré de cohérence d'une communauté épistémique s'apprécie objectivement dans le partage de normes et de statuts professionnels. Anthony Zito rapproche ici la communauté épistémique de l'*advocacy coalition framework* dans la perspective de l'utilisation de la connaissance dans l'influence du politique⁶⁶⁴. Une autre manière de l'apprécier est de comparer la différence de cohésion entre la communauté et les autres acteurs avec lesquels elle se trouve en concurrence⁶⁶⁵. Nous pouvons établir le lien avec la professionnalisation de Mai'a Davis Cross qui intègre une dimension constructiviste sur notamment sur le rôle de réciprocité des dimensions internes et externes à celle-ci⁶⁶⁶. Cette variable cohésion interne de communauté mérite toutefois une forme de relecture à l'aune du rapport à la production et au contexte décrits pour caractériser l'existence de la communauté. La cohérence se mesurerait dans notre approche à la structuration du rapport entre la communauté et la connaissance identifié précédemment.

La cohérence de la communauté est aussi déterminée par la structuration du champ politique concernant l'enjeu. D'une part, cette cohérence est mise en avant par l'existence de données quantitatives fiables sur l'enjeu porté par la communauté (par exemple concernant la sécurité de l'information, le nombre d'attaques sur les systèmes d'information). D'autre part, il y aurait plus de facilité à trouver de la légitimité et du consensus si le problème concerne le système naturel ou l'environnement, au lieu des systèmes sociaux⁶⁶⁷. Autrement dit, pour qu'une communauté ait de l'influence et renforce sa cohérence, elle doit présenter son enjeu comme un enjeu « naturel » plutôt que comme un enjeu « social ». Enfin, la communauté

⁶⁶⁴ SABATIER Paul et WEIBLE Christopher M., « The advocacy coalition framework: Innovation and Clarifications » In. SABATIER Paul, *Theories of the Policy Process*, Oxford, Westview Press, 1999 pp 189 – 222. Voir plus récemment la définition dans SABATIER, Paul « Advocacy coalition framework (ACF) » In, BOUSSAGUET Laurie (dir.), op-cit., 2010, pp. 49-57.

⁶⁶⁵ PETERSON John « Decision-making in the European Union : towards a framework of analysis », *Journal of European Public Policy*, vol. 2, n°1, 1995, pp. 69 – 93.

⁶⁶⁶ RUGGIE John Gerard, « What Makes the World Hang Together? Neo-utilitarianism and the Social Constructivist Challenge », *International Organization*, vol. 52, n°4, 1998, pp. 855-885.

⁶⁶⁷ SABATIER Paul et WEIBLE Christopher M., Op-cit.

semble plus cohérente si elle produit des normes et des objectifs politiques compatibles avec les normes institutionnelles existantes⁶⁶⁸.

C – Discours et communauté épistémique : influence, controverse et concurrence.

Si la communauté épistémique « désigne les canaux par lesquels de nouvelles idées circulent des sociétés vers les gouvernements, et d'un pays à l'autre »⁶⁶⁹, il faut recentrer cette communauté à l'échelle du discours lequel est le principal médiateur d'une idée, laquelle évolue dans son propre espace sémantique⁶⁷⁰. Nous avons retenu que la communauté épistémique se caractérisait à travers des processus finalisés de fabrication et de stabilisation visant une production dynamique de connaissances, de producteurs de connaissance, et corolairement de l'identité communautaire (elle-même liée à l'ordonnancement particulier des connaissances de la communauté). Le point d'émergence communautaire semble être le fait que les connaissances soient employées à des fins politiques. Au-delà de sa mécanique de base, la communauté épistémique peut atteindre divers degrés d'intégration qui déterminent la prégnance de son caractère épistémique par rapport à d'autres caractères, ce sont les trois indicateurs de la communauté épistémique de Mai'a Davis Cross : l'horizontalité du fait communautaire et sa plus-value (le tout formé plus grand que la somme de ses membres), le sentiment d'appartenance partagé, et le partage de normes et valeurs communes. Cette communauté en interaction avec l'extérieur et notamment des décideurs peut disposer d'une influence sur le politique. Son influence est d'autant plus importante lorsqu'elle repose sur l'incertitude des décideurs concernant un enjeu particulier, que cette communauté a accès à ces décideurs, anticipe leurs besoins et leurs actions. Enfin la communauté épistémique doit en quelque sorte imposer sa production de connaissance. Elle peut mieux le faire plus efficacement par la détermination des termes du débat initial et par un lien entre sa connaissance et l'application de la décision plutôt que par les croyances qui fondent celle-ci, ainsi que

⁶⁶⁸ JORDAN Andrew et GREENAWAY John « Shifting Agendas, Changing Regulatory Structures And The ‘New’ Politics Of Environmental Pollution »,: British Coastal Water Policy, 1955–1995. *Public Administration*, 76, 1998, pp. 669-694.

⁶⁶⁹ BOSSY Thibault, et EVRARD Aurélien. « Communauté épistémique », In. BOUSSAGUET Laurie, JACQUOT Sophie et RAVINET Pauline (dir.), *Dictionnaire des politiques publiques. 4^e édition précédée d'un nouvel avant-propos*. Presses de Sciences Po, 2014, pp. 140-147.

⁶⁷⁰ Voir chapitre liminaire et conclusions de l'ouvrage, PASSERON, 1991, pp. 357 – 403.

réciproquement lorsque son degré de cohérence interne dans la production et l'intégration s'adapte aux déterminants extérieurs (professionnalisation).

Dans la perspective que nous retenons, la communauté épistémique ne sert plus à traduire l'influence de tel ou tel groupe sur la prise de décision, mais au contraire à produire l'analyse des (co)variations de sa production, de sa composition et de son influence dans le temps pour mesurer l'influence d'un enjeu dans un vaste ensemble de normes qui dépasse la seule décision ponctuelle. D'un point de vue ontologique, nous considérerons ainsi au travers du discours et de notre grille épistémique que cette communauté désigne le phénomène dynamique de redistribution des rapports de force dans l'espace sémantique relatif à un enjeu (la sécurité de l'information). L'influence de la communauté épistémique traduit la recherche de l'influence d'un discours « logique » dans l'espace sémantique pour comprendre et influencer le monde « historique ».

Il en résulte une controverse discursive entre le discours en question et d'autres compréhensions de celui-ci. La communauté épistémique est donc un espace dynamique de redistribution des rapports de force dans l'espace sémantique entre plusieurs discours autour d'un même enjeu. Rendre compte des frontières conceptuelles d'un discours permet ainsi de dégager les lignes de démarcations, les mutations et les espaces controversés au sein de la communauté épistémique relative à l'enjeu objet de l'analyse. Plus précisément, la communauté épistémique comprise comme une cible mouvante reflète une partie du contexte de l'idée politique qu'elle porte. Conséquence de la co-construction de la communauté, comprendre cette division communautaire revient à admettre une « assortativité » des membres des communautés. Autrement dit, une forme de « préférence » de certains membres de la communauté pour d'autres membres de celle-ci. Cette préférence est la consécration d'un principe hiérarchique au sein de la communauté : En produisant un ensemble hiérarchisé de connaissances, la communauté hiérarchise également les producteurs de cette connaissance. Cette conception nous amènerait à considérer que chaque membre de la communauté épistémique hiérarchise les connaissances et ses producteurs. Néanmoins, il semble y avoir des critères communément admis qui déterminent hiérarchisations donc la production communautaire. Ces différents principes concourent à la production de la hiérarchie dans un contexte où la communauté épistémique apparaît principalement contingente. Si ces divisions affectent la production de la communauté épistémique, elles sont les résultantes à la fois d'éléments relativs à la cohérence de la communauté et à des déterminants extérieurs.

1 – Influence communautaire : des influences « logiques » sur le « monde historique ».

Du point de vue externe, la communauté épistémique opère selon des logiques d'influence à un niveau conceptuel en intervenant dans l'espace de négociation d'une décision politique⁶⁷¹ par la détermination des termes initiaux du débat et éventuellement la production d'« idées nouvelles »⁶⁷². Devant être l'objet d'une méfiance accrue, cette « nouveauté » n'a pas besoin d'être objectivement déterminée mais seulement relativement dans le temps court. Dans cette conception, la communauté épistémique se construit au-delà de toute affiliation institutionnelle de ses membres par les croyances communes de ces derniers dans les origines et les solutions d'un problème qui leurs apparaissent « scientifiquement objectives ». D'un point de vue discursif, il y a une forme de circulation de l'idée depuis l'espace logique vers le monde historique à travers l'espace sémantique.

Comme nous l'avons souligné dans le chapitre liminaire, la connaissance se place hors et dans les murs de la « cité scientifique ». Fondamentalement, la compatibilité de l'énoncé d'une proposition avec le réel se définit dans un espace sémantique. Seule la compatibilité d'un énoncé avec un autre se définit dans l'espace logique. Dès lors la situation d'influence d'une communauté épistémique peut être comprise comme une forme particulière de l'espace sémantique où le langage logique détermine le langage naturel et la compréhension du monde historique. L'influence de la communauté épistémique fonctionne alors de façon analogue au processus scientifique défini par Jean-Claude Passeron. Autrement dit, inclure la dimension discursive revient à brouiller volontairement la frontière entre les deux acceptations traditionnelles de la communauté épistémique⁶⁷³.

A l'inverse, le scientifique ne peut prétendre à la totale maîtrise de l'espace logique. Selon l'approche que nous avons sélectionnée, l'ensemble des contraintes empiriques et historiques qui viennent juger la validité d'une proposition sont formalisées dans l'espace logique. Le scientifique n'a pas le monopole de la connaissance à caractère scientifique. Certes, par sa culture professionnelle, la nature de son activité et sa dénomination, il a une

⁶⁷¹ Pour reprendre la compréhension de l'influence de DRAKE William J., et NICOLAIDIS Kalypso, 1992, op-cit. p. 42

⁶⁷² Ibid.

⁶⁷³ Cf. chapitre liminaire.

prédisposition à œuvrer en la matière mais ne peut revendiquer le monopole de l'expertise. La communauté épistémique peut intégrer d'autres formes d'expertise. Devenir un membre de la communauté épistémique, c'est devenir un producteur de connaissances destinées à être formulées dans le référentiel de l'espace logique.

2 – Des controverses dans la communauté épistémique : concurrence et influence dans l'espace sémantique.

Si l'on admet que la communauté résulte de la co-construction de la production et de l'identité communautaire, cela implique que la pluralité identitaire répond d'une divergence dans la production communautaire. Or, la production d'une communauté épistémique inclut un discours cohérent qui rationnalise la création et l'emploi de son expertise jusque dans l'émergence et la reconnaissance des producteurs de cette expertise. Donc, la pluralité de discours interagit causalement et réciprocement avec les divisions de la communauté. Bien évidemment si la pluralité de discours opère dans l'espace sémantique, la division d'une communauté doit s'entendre du point de vue de la redistribution des rapports de force dans ce même espace. Toutefois, la division communautaire obéit au principe coconstruit de la communauté. De même, l'espace sémantique tient à la fois des langages logique et naturel. Ainsi, la division est aussi une connaissance ordinaire constituée d'assertions qui proposent une description articulée au sein d'un contexte.

Deux observations doivent être désamorcées. La première observation est que l'admission de la division au sein d'une communauté épistémique reviendrait à nier l'existence de celle-ci. C'est sans doute vrai dans une conception classique de la communauté épistémique caractérisée par une forme d'unité de temps et de lieu (une organisation ou un groupe sur un enjeu suite à ou en prévision d'une crise autour d'une décision ponctuelle). Or, dans la conception que nous avons retenu une communauté n'existe pas en un seul endroit, c'est un ensemble dynamique qui peut admettre un certain pluralisme. La seconde observation que la division porterait préjudice à l'influence communautaire dans laquelle devrait exclusivement exister un consensus. Malgré tout, l'option offerte aux décideurs dans le degré ou la nature de la production de la communauté est l'une des capacités qui permet son adaptation, son anticipation. Elle semble être une étape clef dans l'émergence et la stabilisation du processus communautaire. Une communauté qui ne ferait l'objet d'aucune division perd à la fois son horizontalité et son dynamisme.

Les approches défendues par les premiers travaux sur les communautés épistémiques retiennent généralement une influence comprise comme une action de persuasion, laquelle se matérialise par un résultat conforme à la production communautaire. La dimension controversée du discours invite néanmoins à considérer l'influence comme la modification d'un comportement résultant de l'action de la communauté. Deux autres acceptations de l'influence peuvent ainsi être incluses. La première repose sur le phénomène d'imitation. La seconde implique de s'intéresser aux résistances produites par la production communautaire. Il y aurait ainsi trois types d'influence : la persuasion, l'imitation, et la résistance.

L'influence comprise comme une action de persuasion décrit l'hypothèse classique envisagée par la littérature où la communauté parvient à influencer l'acteur qu'elle cherche à influencer. La persuasion peut se déduire d'un cas où un acteur adopte un comportement conforme aux préconisations de la communauté.

L'imitation décrit la situation « accidentelle » où la communauté influence d'autres acteurs que sa cible évidente. Il s'agit d'une forme d'influence obtenue en l'absence d'action de la communauté. L'imitation que la communauté suscite dépasse largement le cadre de son influence et peut également être une notion appliquée à sa production.

La résistance traduit la situation où la production de la communauté suscite une résistance active de la part d'autres acteurs. Cela peut être un acteur que la communauté cherche à influencer ou non. Ce qui caractérise cette influence est qu'elle se déduit des controverses que la communauté rencontre.

Une telle ontologie de l'influence nous permet de caractériser une pluralité de discours au sein d'une même communauté épistémique, et de caractériser une circulation des idées au-delà des frontières de la communauté. Ainsi, la communauté ne procède pas de l'acteur, mais émane épistémologiquement de l'enjeu analysé. Du point de vue de la connaissance, l'enjeu s'alimente non seulement de la production communautaire mais également par la réception de celle-ci. Si nous prenons l'exemple des discussions autour de l'artefact « drone » et de ses usages, il est possible de caractériser l'influence de divers discours lesquelles alimentent la production de la communauté épistémique structurée autour de l'enjeu⁶⁷⁴.

⁶⁷⁴ Sur les perceptions négatives des drones : BOUTHERIN Grégory, « Un nouveau combat pour les UAV ? Quand les drones armés affrontent les perceptions », *Sécurité globale*, n°14, 2010, p. 111-124.

Section 2 - Les frontières normatives de la sécurité de l'information.

Après la relecture de la communauté épistémique vient l'identification des traits communs du discours. Afin de pouvoir dégager des effets communs de discours, il est nécessaire de tracer les frontières entre ce qui peut être admis dans la production du discours et ce qui ne l'est pas. Ces frontières normatives de la sécurité de l'information obéissent à deux ordres : le premier ordre recoupe les frontières intellectuelles qui sont le produit des frontières géographiques traditionnelles, le second recoupe les frontières intellectuelles induites par le contenu du discours.

A - La diffusion de l'enjeu de sécurité de l'information dans le monde.

Si on s'en réfère à au « cyber policy portal » de l'*United Nations Institute for Disarmament Research*⁶⁷⁵, la plupart des États ont mis en place des « documents de stratégie nationale »⁶⁷⁶ ou des lois sur la question de la sécurité de l'information. Il y aurait bien sur des exceptions. Sur le continent Européen, le Kosovo est l'un des seuls États qui n'a pas de stratégie nationale ou de loi. Le Groenland n'aurait pas de documents non plus, mais les questions de défense et de sécurité sont de la compétence exclusive du Danemark qui lui en possède. Au Moyen-Orient et en Asie, la Cisjordanie, le Liban, l'Irak, n'auraient ni loi ni stratégie nationale tandis que l'Iran, l'Ouzbékistan, le Turkménistan, la Corée du Nord, le Vietnam, le Yémen et Taiwan⁶⁷⁷ n'auraient pas de documents de stratégie nationale mais auraient des lois relatives à la sécurité de l'information. Il en va de même sur le continent américain où le Nicaragua et Guyana n'ont pas de documents nationaux. Le Salvador et le Venezuela ont des lois mais ne disposent pas de documents de stratégie nationale. L'Afrique représente le continent où le discours a le moins porté ses fruits au niveau national puisque selon cet observatoire n'auraient aucune loi ou aucun texte de référence la Lybie, le Sahara Occidental, le Soudan, l'Erythrée, la Somalie, le Congo, la République démocratique du Congo, le Gabon, et la Guinée Orientale.

⁶⁷⁵ 194 États font l'objet d'une analyse sur les 197 reconnus par les Nations Unies. Cyber policy portal. Adresse : <https://www.cyberpolicyportal.org/>. Dernière consultation le 17/06/2019.

⁶⁷⁶ Documents officiels conçus pour décrire les positions, les politiques et les stratégies des États afin de résoudre les problèmes liés à la cybersécurité et à la cybersécurité.

⁶⁷⁷ Au sujet de Taiwan, le portail n'indique aucune loi ou document, mais il s'agit ici d'une coquille puisqu'il existe des dispositifs juridiques récents à Taiwan dont notamment le *Cybersecurity Management Act* de 2018. Plus généralement, cela appelle une certaine méfiance sur les oubliés que le portail a pu commettre.

Toutefois, il ne faut pas forcément s'y fier. Si par extraordinaire, les États n'ont pas de textes en interne sur la cybersécurité, ils adhèrent peut-être à une organisation ou à un groupe qui possède ces textes. C'est notamment le cas de l'Union Africaine (UA), de l'Association des nations de l'Asie du Sud-Est (ASEAN), de la Communauté caribéenne (CARICOM), du Commonwealth, de l'Union Européenne (UE), du G7, de l'Union Internationales des Télécommunications (UIT), de l'Organisation du Traité de l'Atlantique Nord (OTAN), de l'Organisation de la coopération islamique (OCI), de l'Organisation pour la Sécurité et la Coopération en Europe (OSCE), l'Organisation des États américains (OEA), l'Organisation de coopération de Shanghai (OCS) et plus généralement comme nous l'avons abordé de manière synthétique (dans notre chapitre 3) de l'Organisation des Nations-Unies (ONU). Autrement dit, la plupart des États sont concernés par une norme en la matière.

De plus, il existe plusieurs conventions internationales spécifiques qui mettent en avant la coopération en matière de sécurité de l'information. Dans l'ordre chronologique de l'ouverture de la signature, on retrouve ainsi, *l'Accord sur la coopération des États membres de la Communauté d'États indépendants dans la lutte contre la criminalité dans le domaine de l'information informatisée* mis à la signature le 1^{er} juin 2001⁶⁷⁸. Le 23 novembre de la même année dans le cadre du Conseil de l'Europe a été mise à la signature la *Convention de Budapest* ou *Convention sur la cybercriminalité*⁶⁷⁹ dont nous avons déjà parlé. Ce sont les deux premières conventions internationales spécifiquement dédiées à la sécurité de l'information. Elles ont pour particularité de mettre en avant la dimension criminelle. Elles ont été rapidement rejoints par le Commonwealth en 2002 qui a mis en place une loi type intitulée *Model Law on Computer*

⁶⁷⁸ La Convention a été signée par tous les États membres de la Communauté des États indépendants sauf la Mongolie (membre observateur de l'organisation) et la Géorgie (ancien membre de l'organisation). Le titre indiqué en traduction. Le titre original de la convention est « Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации ».

⁶⁷⁹ L'ensemble des signataires de la convention étant composé d'États membres du Conseil de l'Europe mais aussi de non-membres car la convention était ouverte. : Albanie, Allemagne, Andorre, Argentine, Arménie, Australie, Autriche, Azerbaïdjan, Belgique, Bénin, Bosnie Herzégovine, Bulgarie, Cap-vert, Canada, Chili, Colombie, Costa Rica, Croatie, Chypre, République Tchèque, Danemark, République Dominicaine, Estonie, Finlande, France, Géorgie, Ghana, Grèce, Hongrie, Islande, Irlande, Israël, Italie, Japon, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Ile Maurice, Mexique, Moldavie, Monaco, Monténégro, Maroc, Pays-Bas, Nigeria, Macédoine, Norvège, Panama, Paraguay, Pérou, Philippines, Pologne, Portugal, Roumanie, Royaume-Uni, Russie, Saint Marin, Sénégal, Serbie, République slovaque, Slovénie, Afrique du Sud, Espagne, Sri Lanka, Suède, Suisse, Tonga, Tunisie, Turquie, et enfin l'Ukraine.

and Computer Related Crime valable dans ses 53 États membres. Cela clôture une première vague de conventions multilatérales.

Une deuxième vague de conventions se met en place entre 2009 et 2014 et marque l'entrée des grandes alliances militaires sur la thématique. Le premier texte est l'*Accord de coopération dans le domaine de la sécurité internationale de l'information* mis en place le 16 juin 2009 par l'Organisation de coopération de Shanghai. L'Organisation du traité de l'Atlantique a intégré la cyberdéfense dans son *Concept stratégique* de 2010 mais n'a pas produit de convention spécifique (sinon que l'adoption du nouveau concept représente la vision commune des États membres de l'OTAN puisque l'organisation fonctionne sur la base du consensus). La *Convention de l'Union Africaine sur la cybersécurité et la protection des données personnelles* a été mise en place le 27 juin 2014⁶⁸⁰. En parallèle de cette deuxième vague, d'autres organisations régionales ont produit leurs propres conventions notamment la Communauté d'Afrique de l'Est en mai 2010, la Ligue des États Arabes en décembre 2010, la Communauté économique des États de l'Afrique de l'Ouest en aout 2011, la Communauté caribéenne en 2012 ainsi que la Communauté de développement d'Afrique australe en novembre 2013.

A ce jour, la dernière vague de conventions multilatérales est notamment marqué par deux textes particuliers. Le premier est la *Déclaration de Brazzaville* du 24 novembre 2016 formulée dans le cadre de la Communauté économique des États de l'Afrique centrale et qui vise l'adoption de lois types sur les télécommunications, la cybersécurité et le cadre réglementaire régissant l'interconnexion transfrontalière. Et de l'autre côté de la Mer Méditerranée, dans l'Union Européenne, le second texte marquant est la *Directive Network and Information System Security (NIS)* du 6 juillet 2016. Si la deuxième vague présente des conventions plutôt orientées vers une forme de coopération, cette troisième vague a pour particularité de présenter des dispositifs qui favorisent davantage la logique de l'intégration.

Nous n'aborderons pas l'ensemble des textes concernés ici. Un tel travail représenterait sans doute un objet de recherche spécifique en soit. Même s'il faudrait sans aucun doute

⁶⁸⁰ Fin avril 2019, cette convention était signée ou/et ratifiée par le Bénin, les Comores, le Congo, le Ghana, la Guinée-Bissau, la Guinée, l'île Maurice, le Mozambique, la Mauritanie, la Namibie, le Rwanda, le Sénégal, la Sierra Leone, Sao Tomé-et-Principe, le Tchad, le Togo, la Tunisie, la Zambie.

développer une analyse du contenu de ces textes et de ces conventions au-delà du seul inventaire (Ce que nous n'avons pas pu faire de façon logométrique pour des raisons de différence de référentiel linguistique), il faut souligner que les divers éléments mis en place permettent de conclure à une progression du phénomène de sécurisation et à une relative omniprésence de celui-ci à travers le monde en dépit des différences dans l'accès aux technologies de l'information.

1 – Des frontières plus étendues que les limites imposées par la technique.

La première chose à constater lorsqu'on examine la diversité et le nombre des textes disponibles, c'est de réaliser que la sécurité de l'information est un enjeu admis, consacré par l'écrasante majorité des États existants soit directement, soit indirectement par le biais d'une organisation internationale ou d'une convention à laquelle ils adhèrent.

D'un point de vue externe, la « géographie normative » de l'information ne semble ainsi pas correspondre à la répartition inégale des moyens techniques de l'information et aux pratiques de l'information. Les technologies de l'information sont donc un enjeu de sécurité peu importe que 40% ou 90% de la population ait accès à Internet (39.8 % en Afrique, 86.8% en Europe en juin 2019⁶⁸¹). Peu importe également le nombre d'Internauts ou peu importe les différences technologiques. La différence technologique renvoie à l'inégalité des réseaux de communication entre les États et à l'intérieur des États en termes de structure et de débit. Le nombre de câbles sous-marins d'un État côtier ne semble pas avoir d'incidence sur la prise en compte sécuritaire de l'information, de même que les différences de standards dans la couverture mobile (3G/4G/5G). Les différences de débit moyen d'un État à l'autre n'engendent pas non plus de différence du point de vue de la diffusion de l'enjeu de sécurité.

D'un point de vue interne au discours, la diffusion de l'enjeu de sécurité de l'information ne souffre pas non plus d'obstacle en termes de vocabulaire. Que l'acteur le désigne comme étant un problème « cyber » ou emploie d'autres termes. On peut néanmoins noter le fait

⁶⁸¹ Chiffres de l'Internet World Stats publiés le 30 juin 2019 sur le site www.internetworkworldstats.com. Dernière consultation le 03/07/2019.

majoritaire du vocabulaire « cyber » tant dans les contextes nationaux que dans le cadre des dispositifs multilatéraux.

Les différences de prise en compte de l’information comme enjeu de sécurité ne semble ni fondée sur le langage, ni sur la technique, mais semble plutôt être le fruit des différents contextes politiques régionaux et nationaux. Si nous prenons l’exemple de la sécurité des informations personnelles des utilisateurs, les différences dans la diffusion et le degré de protection reflètent davantage les différences dans la culture de la vie privée que les différences techniques ou sémiotiques entre les régions du monde⁶⁸². La question posée est ainsi de savoir comment dans toutes ses composantes le contexte politique d’un État influence la production du discours.

2 – Le poids du contexte national dans la production des communautés épistémiques.

Il y a des différences dans la production de connaissance qui sont principalement liées à ces différences de contextes académiques nationaux⁶⁸³ dont le poids est tout aussi fort voir plus fort que les considérations épistémologiques. Sur le fond, il n’y a pas *a priori* de discontinuité entre les compréhensions de la sécurité de l’information et la sécurité de manière générale. La sécurité de l’information s’inscrit néanmoins dans la continuité du comportement des acteurs. Et l’acteur référent en matière de sécurité demeure l’acteur régional, y compris avec l’essor économique des opérateurs privés⁶⁸⁴, y compris dans les enjeux internationaux de sécurité : L’État demeure le prisme à partir duquel et dans le cadre duquel se pense la question de la sécurité. Cela se vérifie y compris dans les discours de l’Union Européenne et de

⁶⁸² Seuls environ 80 États sur 197 ont une loi spécifique qui concerne la vie privée et la protection des données hors les rares cadres multilatéraux.

⁶⁸³ Pour le cas des Relations Internationales par exemple, voir BALZACQ Thierry et RAMEL Frédéric, 2013, op-cit, pp. 31-268.

⁶⁸⁴ Dans une perspective critique voir en plus des ouvrages déjà présenté : DIAZ, Frédéric. « « coproduction » de la sécurité : une nouvelle forme de l’interventionnisme étatique pour une meilleure sécurité du public ? (le cas de grands rassemblements de populations en france) », *Déviance et Société*, vol. 27, no. 4, 2003, pp. 429-458.

l'ONU⁶⁸⁵. Même le concept d'autonomie concernant Internet se forme principalement et historiquement à partir du référentiel de l'État⁶⁸⁶.

Notre idée initiale était qu'il existait une division au sein des communautés épistémiques entre les membres dans les liens qui les rattachent à l'un ou l'autre des contextes nationaux. Ce rattachement tient à la fois des liens bureaucratiques et des objectifs des divers discours au sein de la communauté épistémique elle-même. Cette division est apparue clairement lors de l'ouverture du terrain en novembre 2012. Mais il est également apparu que l'apparente position privilégiée de l'acteur régional pouvait paradoxalement montrer les phénomènes d'influence entre États sur cette question précise à travers les influences sur la production de la communauté épistémique.

Pour appartenir à la communauté discursive « cyber » il faut que les discours produit soit compatible avec une forme de demande régionale qui varie en fonction de l'État concerné. Dans la plupart des États, l'appareil gouvernemental produit une demande forte de connaissances nouvelles en matière de sécurité de l'information. L'importance de l'acteur public dans le financement de la recherche soit est d'ailleurs un élément important de cette demande. Cette préoccupation inscrit la plupart des comportements politiques internationaux en matière de cybersécurité dans une forme de prolongement des comportements existants mais qui impacte profondément la confiance des acteurs quels que ce soit le niveau auquel on se situe.

Dans une série d'entretiens réalisés avec le personnel du Ministère des affaires étrangères français⁶⁸⁷ l'idée de développer la confiance avec les autres États a été soulevées à plusieurs reprises. Cette question de la confiance en matière de sécurité de l'information semble également importante dans les coopérations internationales en matière de production communautaires. De manière générale, l'idée de travailler dans le secteur de la sécurité de l'information ou d'en faire son objet de recherche est perçue comme non-neutre dans les

⁶⁸⁵ Cf. Chapitres 3.

⁶⁸⁶ LOVELUCK Benjamin, op-cit.

⁶⁸⁷ Notamment, le 9 juillet 2014, avec le secrétaire des affaires étrangères chargé de la cybersécurité à la direction générale des affaires politiques et de sécurité du Ministère des affaires étrangères (entretien semi-directif réalisé dans les locaux du ministère), ainsi que le 9 juin 2015 avec le directeur adjoint des affaires stratégiques, de sécurité et du désarmement de la direction générale des affaires politiques et de sécurité du Ministère des affaires étrangères, entretien déjà cité.

rapports entre français et étrangers⁶⁸⁸. Du point de vue de la recherche, il y a une forme d'ambiguïté qui affecte le monde de la recherche entre le poids perçu de l'intérêt national et le marché international qui est le sien. Il y a une forme d'ambiguïté qui affecte les autres acteurs publics ou privés à l'égard du monde académique entre le caractère confidentiel ou réputé confidentiel des informations et l'ouverture de la pratique scientifique par la valorisation de la recherche.

La rhétorique du soupçon qui anime les débats autour des récits évoqués en introduction ainsi que sur d'autres exemples aboutit à un climat de manque de confiance perceptible à la plupart des niveaux. Les données statistiques et l'analyse de discours doivent ici être complétées avec quelques éléments issus des entretiens réalisés au profit de cette thèse. Interrogé sur le point de savoir comment construire la confiance entre deux nations avec différentes cultures et différentes armées, la première réponse du directeur de la *National Security Agency*, militaire issu de l'*US Navy*, a été de dire que cette question lui était posée car « les États-Unis étaient pris pour un adversaire »⁶⁸⁹.

B – La différenciation par le contenu des discours.

Les frontières des discours nous renseignent sur les principales lignes de démarcations conceptuelles au sein de la communauté épistémique de la sécurité de l'information en France. En tant que cible mouvante, la communauté épistémique doit admettre une forme d'altérité. Cette altérité est symbolisée par des divisions qui fondent les critères de celles-ci. Là où les critères traditionnels de la communauté épistémiques mettent l'accent sur ce qui rassemble la communauté, la division prend sa source dans tout ce qui peut entraîner des différences et des transformations de la production communautaire. On se demande alors comment la communauté épistémique existe malgré les divisions qui la poussent à la séparation. A l'échelle de la communauté épistémique, nous rejoignons ici la sociologie des organisations et la théorie

⁶⁸⁸ L'idée de travailler avec le ministère de la défense est apparue comme non-neutre et pouvant engendrer des réactions de méfiance vis-à-vis de la recherche internationale. Ce fait est particulièrement ressorti lors de deux entretiens. Le premier, avec un ingénieur de nationalité allemande militant anarchiste du Chaos Computer Club le 13 mars 2014 à l'occasion du colloque « Le monde après Snowden » organisé par la chaire Castex, rue de l'université à Paris. Le deuxième, avec un Ingénieur d'Études au CNRS, titulaire d'une chaire de recherche du ministère de la défense, le 11 juillet 2014, au bar Ciel De Paris, Tour Montparnasse, Paris.

⁶⁸⁹ Extrait de notes d'un entretien collectif réalisé le 16 juillet 2015 à l'Ecole Militaire Paris avec le directeur de la NSA et du US CYBER Command par les membres du séminaire jeunes chercheurs de la chaire Castex.

de l'acteur stratégique dans laquelle chaque acteur agit pour améliorer sa capacité d'action en relative autonomie⁶⁹⁰. Cela suppose ontologiquement que les buts de la communauté épistémique (influence des normes) peuvent être différent des buts de ses membres. L'approche de cette théorie examine une organisation à travers les rapports de pouvoir qui la structurent.

Sous la multiplication et la diffusion des termes dérivés du cyberspace, se caractérise une forme de discours construit autour d'une convergence entre les enjeux de sécurité de l'information, l'intérêt régional et le langage. Comme affirmé dans le chapitre premier, l'idée de sécurité appliquée à l'information comme un intérêt régional est présente dès les origines du cyberspace dans la littérature de science-fiction. Cette association est avant tout consacrée au point de vue du langage par l'association du terme « cyberspace » puis de ses dérivés spécifiquement à l'idée de sécurité de l'information pour traiter des questions politiques. Cette convergence d'idées ne peut fonctionner qu'en présence de deux associations antérieures « sécurité de l'information – Cyber » dont nous venons de parler, mais surtout « Sécurité de l'information – État ». Ce n'a qu'à raison de l'inscription du langage « cyber » dans le prolongement de l'intérêt régional pour l'information comme objet de sa sécurité que le discours analysé peut exister sous sa forme actuelle.

La communauté discursive construite autour du cyberspace et de la sécurité de l'information peut se définir selon trois critères particuliers que sont l'emploi du label « cyber » (critère formel), une conscience des enjeux de la sécurité de l'information (critère matériel), et une position particulière vis-à-vis de la demande sociale pilotée par l'acteur étatique (critère politico-organique). Pourrait ainsi être membre de cette communauté, une personne qui : Utilise un lexique composé de cybermots, pour parler de sécurité de l'information, en accord avec un cadre étatique.

Toute la communauté discursive repose sur le triptyque « sécurité de l'information – cyber – État ». Ces critères sont cumulatifs et favorisent des logiques d'inclusion et d'exclusion de la communauté : une personne qui parle de sécurité de l'information, en accord avec un cadre étatique sans employer un mot « cyber » ou l'employant « mal » se disqualifie comme spécialiste de la thématique. Une personne qui utilise les cybermots en accord avec un cadre étatique sans pour autant parler de sécurité, aura une approche perçue comme moins légitime

⁶⁹⁰ CROZIER Michel. et FRIEDBERG Erhard, (1977). Op-cit. Voir également DION Stéphane. « Erhard Friedberg et l'analyse stratégique », *Revue française de science politique*, 43^e année, n°6, 1993. pp. 994-1008.

de l'enjeu. Une personne qui utilise un cybtermot pour parler de sécurité tout en refusant le cadre défini à partir de l'État comme référentiel sera perçu comme un adversaire de la communauté, vecteur d'insécurité.

1 – Les frontières induites par le discours « sécurité de l'information – cyber – État » : critères matériel et formel.

Le critère matériel d'appartenance à la communauté discursive repose sur le fait que l'information est un objet de sécurité, quelle que soit sa structure, quelle que soit sa forme, quelle que soit son support. Cela dépasse la sécurité des systèmes informatiques, la sécurité de l'information sous forme numérique ou les autres sous-domaines de la sécurité de l'information. Cette idée de sécurité représente le consensus minimal autour duquel l'ensemble des acteurs s'entendent pour créer des espaces de dialogues entre des communautés préexistantes. « Cyber » s'entend donc ici au sens strict de « cybersécurité » ou « cybercriminalité », voire parfois de sécurité des personnes (« cyberdépendance », « cyberharcèlement »). Quoique cette dernière thématique apparaisse de manière secondaire dans les thématiques de recherche observées. Ce critère produit rapidement une double-exclusion : il exclue du discours toute personne qui emploient les « cybtermots » (critère formel) pour parler d'autre chose que de la sécurité (ce qui favorise la contestation dans la communauté) ainsi que toute insertion de la sécurité dans un ensemble plus vaste. Cette idée de sécurité doit s'entendre au sens de sécurité informatique et non pas au sens de sécurité générale. Cela aboutira à l'exclusion relative du discours « cyber » des enjeux numériques entendu plus largement, y compris par les acteurs de communauté.

L'emploi du marqueur exclu la plupart des compréhensions autre que « sécuritaires » et au sein de celles-ci à une sécurité principalement technique. Cette idée de sécurité informatique est fondamentale pour comprendre la hiérarchisation de la thématique et la manière dont elle structure sa communauté d'emploi. Un bon emploi du marqueur « cyber » est donc nécessairement marqué par cette idée de sécurité informatique et pourrait probablement se voir classer selon une double-échelle : thématique (sécurité informatique et sécurité générale) et chronologique (avant / après la réalisation de la menace). La hiérarchisation des emplois en termes de légitimité résidant alors dans une présomption de compétence alloué à certaines disciplines pour parler d'un type de problème. Sur une thématique proche de la sécurité informatique, les sciences informatiques apparaîtront plus légitimes pour protéger

l'information, après l'attaque les sciences informatiques et/ou techniques apparaissent moins pertinentes au-delà des quelques tâches de réparation qui leur sont nécessairement dévolues. Tandis que d'autres domaines de connaissances telles que le droit, l'économie, la gestion, la politique sont jugées a priori plus pertinentes pour examiner les conséquences de la réalisation de la menace.

Les problématiques liées aux macro-données (*big data*), aux données personnelles, à l'accès à Internet, ne peuvent recevoir légitimement l'indicatif « cyber » qu'à raison de la possibilité d'un mésusage ou d'une défaillance technique liée à la sécurité informatique. La sécurité vient opérer une forme de concentration sur quelques mots-clefs et une perte d'amplitude dans les néologismes employés. Le cyberspace compris ne sert plus à décrire tout ce qui est relatif à Internet et aux technologies de l'information. La conception de la sécurité défendue semble assez particulière d'un point de vue extérieur. En effet, constitue un risque légitime par exemple la soustraction frauduleuse des informations d'une carte bancaire avec son dispositif RFID ou du fait d'un automate bancaire défaillant ou piraté, mais ne serait pas légitimement susceptible d'être analysée en cas de perte de la carte par l'utilisateur.

Il y aurait ainsi une forme de discontinuité entre sécurité informatique et sécurité de l'information. La première ne se concentrerait que sur le volet informatique, tandis que la seconde engloberait toutes les dimensions de l'information dans ses aspects informatiques, mais aussi physiques. Une lecture plus fine invite à relativiser cette distinction. Il y aurait ainsi de l'information numérique et de l'information physique (ou analogique). De plus, parmi les choses numériques, il y aurait curieusement de l'information numérique et d'autres choses qui ne sont pas à proprement parler de l'information (quand bien même ces choses demeurent vulnérables par l'information). Cette double échelle invite dès lors à distinguer trois domaines de sécurité en apparence bien défini : la sécurité de l'information, la sécurité des systèmes d'information et la cybersécurité. La première s'occuperait d'information, la seconde concernerait uniquement l'information numérique, et la troisième s'intéresserait à tout ce qui est numérique même si ça n'est pas de l'information. Reposant largement sur la confusion entre données et informations ce type de distinction vient conditionner une capacité à segmenter trois types de communautés qui ont pour lieu commun le fait de définir l'information comme objet de sécurité sans toutefois avoir le besoin du label « cyber » pour définir leur activité. Si bien que le label trouve également une nouvelle importance qui rassemblera ou divisera les experts sur des stratégies individuelles plutôt que sur les concepts en question.

Il convient également d'évoquer le « numérique ». Ces dernières années, dans l'administration comme dans le milieu de la recherche, il y a eu des appels pour récuser la cybersécurité au profit de nouvelles appellations : la sécurité numérique, la sécurité à l'ère numérique, la sécurité des données (numériques), le risque numérique... Cette dernière appellation vient compléter tout un panel de domaines déjà existant en mimant toutes les difficultés conceptuelles là où elle prétendait les gommer. L'intérêt majeur de cette nouvelle appellation consiste principalement à pouvoir diffuser et promouvoir l'idée de sécurité sur un terrain nouveaux : celui des enjeux qualifiés de numériques. Autrement dit, cela revient à intégrer et développer un langage nouveau compatible avec l'image positive véhiculée par le terme « numérique » là où le « cyber » est connoté négativement.

Jusqu'à très récemment en France, les enjeux de sécurité liés à l'information existaient un peu à part des autres enjeux de l'information. Le langage spécifique constitué par le marqueur « cyber » en était un exemple... Mais plus généralement, lorsqu'était envisagé le rôle de l'information dans les échanges de cultures, ou de l'économie, la plupart des auteurs avaient plutôt une image positive de ces technologies : pas de risque sécuritaire pour l'utilisateur, pas de problème de manipulation de l'information, pas de problème d'hégémonie technologique d'un État sur un autre... Cette forme d'impensé de la sécurité ne doit pas être attribué à une ignorance, mais plutôt à un choix délibéré. Ce choix est le fruit d'une opposition entre approches « technophiles » et « technophobes ». En effet, il est moins difficile de vanter les mérites d'une économie numérique en éludant les failles de la sécurité informatique. Pourtant ces deux domaines ont une chose en commun : la diffusion des technologies. Cela serait évident si les gens posaient un regard neutre sur la technique, or il semble y avoir une césure entre des postures technophiles et technophobes. La sécurité relèverait d'une posture technophobe opposée aux enjeux numériques plutôt inspirés d'une posture technophile : la gouvernance, l'éducation, la liberté, la modernité, l'innovation, l'accessibilité... Les technologies de l'information n'apparaissent pas neutres dans un langage qui est destiné à assurer leur promotion dans l'ensemble des milieux de la société. L'inverse un discours qui vanterait des valeurs positives d'une sécurité amoindrie s'attirera un regard négatif de la part des porteurs de la thématique de la sécurité. Du point de vue du terrain de cette recherche, ce phénomène s'illustre assez bien dans les espaces dédiés aux questions dans les colloques scientifiques et dans les conflits qui sont mis en avant par certaines de ces questions.

Un autre critère, purement formel, pourrait être formulé ainsi : « Peut être membre de la communauté, toute personne qui emploie le vocabulaire composé de cyber-mots ». La maîtrise du vocabulaire et l'affichage sous le label « cyber » détermine ici une volonté d'appartenance d'un acteur donné à une communauté donnée. Corolairement, refuser les « cyber-mots » du lexique peut être un facteur d'exclusion de la communauté ou comme un jugement négatif sur celle-ci. Parler d'un label « cyber » est évidemment abusif dans la mesure où en France, le label est un terme qui désigne une mention officielle.

Le lexique est vécu principalement comme un facteur de différenciation dans une communauté plus large qui est la communauté d'origine de l'acteur ainsi comme un vecteur de dialogue entre d'autres ensembles. Ainsi au travers du lexique, la communauté « cyber » peut être regardée comme un croisement d'acteurs issus de l'ensemble des composantes d'une société donnée. Cela se traduit notamment par deux aspects : l'association du langage à la sécurité et le caractère disparate de la communauté « cyber ». Lesquels produisent une contestation autour du discours qui rend difficile la compréhension de la frontière entre le qualificatif et ce qu'il désigne ; autrement dit, entre ce qui peut être reconnu comme « cyber », et ce qui ne peut pas l'être. Ce recours au label n'est possible que dans la mesure où la communauté discursive partage l'idée qu'il sert avant tout à parler de l'information comme un enjeux de sécurité collective et/ou individuelle. Toutefois, ce sens n'est pas la représentation dominante du cyberspace entre sa création et sa transition vers le vocabulaire de la sécurité. Autrement dit, derrière l'association de l'affixe « cyber » à la sécurité se cachent plusieurs autres communautés avec leurs propres concepts.

Qui emploie le langage « cyber » pour parler de sécurité ? Quels étaient les domaines d'expertise ou de recherche des personnes qui ont employé ce nouveau langage ? Le travail de terrain sur cette thèse a été l'occasion de rencontrer des industriels, des chercheurs, des institutionnels issus de différents domaines. Il est possible de classer les profils entre deux catégories, des profils généralistes pour qui il s'agit d'une thématique périphérique et des spécialistes qui appliquent à la sécurité de l'information la grille de lecture issus de leurs domaines et/ou thématiques respectifs. Tout utilisateur peut être intéressé. Les secteurs concernés peuvent être les transports, finances, industries, santé, énergie, informatique, télécommunication, médias, administrations civiles et militaires et bien évidemment l'enseignement et la recherche. Sur ce dernier aspect, les disciplines académiques sont

relativement nombreuses⁶⁹¹. Les catégories socio-professionnelles des personnes rencontrées sont également très diversifiées. Se retrouvent ainsi l'ensemble des cadres et professions intellectuelles supérieures (professions libérales, cadres de la fonction publique, professeurs, professions scientifiques, Professions de l'information, des arts et des spectacles, cadres administratifs et commerciaux d'entreprise, ingénieurs et cadres techniques d'entreprise), mais aussi des personnes issues professions intermédiaires administratives de la fonction publique, des professions intermédiaires administratives et commerciales des entreprises, des techniciens, des employés civils et agents de service de la fonction publique, des policiers et militaires, des étudiants, des retraités... Sauf exceptions, les principaux intervenants de la communauté ont un niveau de formation élevé compris entre Bac +3 et Bac +5 et plus, avec une forte présence de formations équivalent Bac+5 (Master / DEA / DESS, diplômes d'ingénieurs ou équivalents). Pour la plupart des structures représentées dans les événements de la communauté, les personnes présentes sont déjà identifiées comme des spécialistes ou futurs spécialistes de la thématique pour la structure dont ils sont membres. La majeure partie des personnes rencontrées au cours de ces manifestations étaient des hommes. Le nombre de femmes diminue avec l'accroissement du niveau de responsabilité, y compris dans le milieu de la recherche.

Cette pluralité de domaines, de secteurs et de profils entraîne une lisibilité difficile des thématiques que les variations du cyberspace peuvent décrire. Le phénomène discursif s'est parfois frayé un chemin jusqu'aux concepts. La cyberdéfense par exemple, fortement liée aux acteurs militaires, est un concept qui correspond à un ensemble d'acteurs, de pratiques et d'interactions formalisés et facilement identifiables⁶⁹² (contrairement la cybersécurité et à la cybercriminalité qui demeurent des domaines plus vagues). Un autre exemple est celui du système cyber-physique⁶⁹³ qui décrit un système de coopération entre outil informatique, Internet et utilisateur. Le système cyber-physique en tant que concept peut servir à décrire de

⁶⁹¹ En résumé des spécialistes issus de disciplines : Droit, Criminologie, Science Politique, Sciences économiques, Sciences de gestion, Sciences du langage, Psychologie, Philosophie, Sociologie, Anthropologie, Histoire, Géographie, Urbanisme, Mathématiques, Informatique, Génie informatique, Neurosciences, Sciences de l'éducation, Sciences de l'information et de la communication...

⁶⁹² Voir l'ouvrage récent TAILLAT Stéphane, CATTARUZZA Amaël, DANET Didier, *La Cyberdéfense - Politique de l'espace numérique*, Paris, Armand Collin, juillet 2018, 357 p.

⁶⁹³ LEE Edward, A., « Cyber-Physical Systems - Are Computing Foundations Adequate? », Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, Austin, Texas, octobre 2006.

façon transdisciplinaire des systèmes autonomes (drone, automobile) mais également des procédés de réseau intelligent de distribution d'électricité ou d'imagerie médicale.

Les autres thèmes demeurent finalement assez notionnels, à moins de se soustraire à l'emploi du lexique « cyber ». On observe souvent un décalage entre l'usage du terme propre à décrire « l'enjeu » et les concepts scientifiques et opératoires mobilisés en pratique. Ce décalage est interprété comme une forme de transformation en label du phénomène discursif qui vient sanctionner tel ou tel objet préalablement défini sans y rechercher de dimension conceptuelle. La traduction du « label » en concept déminuant sans doute le pouvoir évocateur de ce dernier. Du point de vue de la recherche, cette idée décrit la quête du signe d'une qualité particulière la production à caractère scientifique. En soit, le phénomène discursif « cyber » est un signe qui donne une valeur particulière à la recherche. Cette valeur se construit autour de plusieurs idées que sont la modernité, la lutte contre l'insécurité et l'amélioration de la technique. Cette valorisation construit un effet marketing autour du discours « cyber ». La labellisation se conçoit avant tout comme un outil de promotion d'une production. Dès lors, pour la recherche, la question de la posture du chercheur est posée. N'y a-t-il pas une forme d'opportunisme à vouloir appliquer un label à un concept scientifique qui lui est totalement étranger ? La question pourrait sembler iconoclaste si elle ne structurait pas une grande partie des débats internes à la communauté, particulièrement dans les concurrences de légitimité entre disciplines académiques⁶⁹⁴. Ces questions illustrent un champ discursif en proie à de nombreuses contestations qui ne facilitent pas vraiment la délimitation d'objets scientifiques.

2 – Les liens bureaucratiques comme source de division au sein de la communauté.

Si la première source de division qui vient à l'esprit pour la communauté épistémique concerne la connaissance. Cette source résiderait dans les structures et les processus qui entourent la connaissance à caractère scientifique de sa production à sa reconnaissance. Nos développements antérieurs indiquent toutefois que ce n'est pas tant une affaire de connaissance que d'intégration communautaire. La principale source de division au sein d'une communauté

⁶⁹⁴ Du point de vue du discours, cela entraîne parfois une contestation, parfois publique, de l'application de l'étiquette. En grossissant le trait, on pourrait résumer la contestation à la négation du label sur un ton péremptoire qui confine parfois au caricatural : « Ce n'est pas 'cyber' ». Allégation entendue avec quelques variantes de nombreuses fois au cours du terrain.

épistémique est celle qu’entraîne la solidarité des « liens bureaucratiques » entre les membres de la communauté. Porté à l’échelle collective, il y a une « concurrence bureaucratique » entre les membres d’une même communauté épistémique. Cette concurrence suppose un principe de hiérarchisation des connaissances où chaque membre de la communauté favorisera les membres de la communauté qui sont déjà « plus proches » de lui (avec qui la personne entretient déjà le plus de liens). La force de ce lien de déduit de l’importance des trois critères d’intégration communautaire utiles pour la reconnaissance de la communauté. Pour rappel, ces trois indicateurs reposent sur le décloisonnement des cadres bureaucratiques au profit des échanges et de la construction d’une culture professionnelle commune. Dès lors les liens bureaucratiques entre les membres d’une même communauté épistémique représentent la principale source de division au sein de celle-ci. Pour comprendre ce lien bureaucratique, il est possible de faire appel à plusieurs conceptions de la bureaucratie. Les travaux sur les communautés épistémiques renvoient généralement à des conceptions proches d’une conception wébérienne de la bureaucratie. La direction administrative bureaucratique de Max Weber définit un idéal-type de la domination légale⁶⁹⁵. Ce modèle représente une forme de monarchie perçue comme le contraire de la « collégialité ». Les individus qui la composent sont personnellement libres, n’obéissent qu’aux devoirs objectifs de leur fonction, dans une hiérarchie de la fonction solidement établie, avec des compétences de la fonction solidement établies, en vertu d’un contrat, payés par des appointements fixes. Ces individus traitent leur fonction comme unique sinon principale profession et s’inscrivent dans un mécanisme de carrière déliés de leur emploi et des moyens de l’administration. Enfin, ils sont soumis à un contrôle et à une discipline stricte et homogène.

Michel Crozier⁶⁹⁶ reprend cette idée d’impersonnalité des règles mais en renonçant au caractère rationnel de celles-ci. Il décrit la bureaucratie comme un phénomène implicite qui fournit un minimum acceptable de protection des individus à la coordination des activités coopératives nécessaires à la réalisation des objectifs de leurs objectifs. L’un des apports de son travail réside dans le concept de « zone d’incertitude » qui permet l’existence de lutte pour le

⁶⁹⁵ WEBER Max, *Économie et Société*, Paris, Plon, 1971, 410 p.

⁶⁹⁶ CROZIER Michel. *Le phénomène Bureaucratique : Essai Sur Les Tendances Bureaucratiques Des systèmes D’organisation Modernes Et Sur Leurs Relations En France Avec Le systèmes Social Et Culturel*, Paris, Ed. Du Seuil, 1993, 413 p.

pouvoir. À l'échelle de l'individu, l'enjeu est de maîtriser sa zone d'incertitude afin de gagner en pouvoir et en autonomie. La bureaucratie constitue :

« Un système d'organisation incapable de se corriger en fonction de ses erreurs et dont les dysfonctions sont devenues un des éléments essentiels de l'équilibre »⁶⁹⁷.

Le lien bureaucratique comme limite de la communauté épistémique s'entend alors non seulement comme le fruit des rapports de pouvoir pesant sur les individus, mais également dans une dimension systémique dont le « dysfonctionnement » (caractérisé comme un mauvais fonctionnement d'un cycle d'information entre les erreurs et leurs corrections) permet à la communauté épistémique d'exister.

Si les divisions de production peuvent s'établir à l'aune de toute variable qui affectent négativement l'intégration communautaire : phénomènes de concurrence, intérêts nationaux différents, éloignement géographique, disciplines et revendications académiques opposées, référentiels linguistiques et culturels différents... La plupart de ces divisions trouveront source dans ces liens bureaucratiques. A partir de cette lecture et des éléments relatifs à la communauté discursive, nous pouvons établir trois grandes divisions qui structurent une communauté épistémique de la sécurité de l'information.

C – Influences politiques au sein de la couche technique d'Internet.

Evoquer les débats politiques relatifs à la couche technique d'Internet revient souvent à accréditer la thèse d'une forme de domination d'Internet rendue possible par la technique. Selon cette approche, les États-Unis dominent Internet par les normes, la gouvernance ou de l'infrastructure du réseau. Cela produit souvent une situation un peu confuse où un Internet, très décentralisé dans ses représentations devient paradoxalement très centralisé.

Dans un premier temps, nous résumerons le caractère politique de la gouvernance d'Internet et démontrerons son caractère centralisé aux États-Unis, avant de contrebalancer cette assertion par l'un des exemples de production de sécurité d'Internet au travers des *Computer Security Incident Response Team* (CSIRT). L'enjeu de cette sous-section est de

⁶⁹⁷ Ibid. p. 257.

démontrer que le caractère politique d'Internet ne se limite pas aux relations interétatiques mais touche également sa dimension technique.

1 – Gouvernance et controverses du contrôle technique d'Internet.

Cette question de la gouvernance d'Internet est fondamentale pour comprendre la majeure partie des enjeux politiques et scientifiques qui structurent l'information, y compris au-delà des aspects de sécurité. Il s'agit d'un processus long démarré en 1979 avec la DARPA⁶⁹⁸ et dont le Sommet mondial sur la société de l'information organisé par l'Union internationale des télécommunications à partir de 2003 représente l'une des dernières formes⁶⁹⁹. Si l'on reprend la définition dudit sommet⁷⁰⁰, la gouvernance désigne « l'élaboration et l'application conjointes, par les États, le secteur privé, la société civile et les organisations internationales, dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décision et programmes propres à façonner l'évolution et l'usage de l'Internet »⁷⁰¹. Cela veut dire que la gouvernance s'occupe ainsi des questions relatives à l'infrastructure et à la gestion de ressources Internet critiques (normes techniques, gestions des adresses IP, des noms de domaine, des systèmes de communication, des langues...), mais aussi les questions relatives à l'utilisation de l'Internet, y compris la délinquance, le commerce international, la propriété intellectuelle ainsi que le développement des capacités pour les États qui ont accès plus limité à Internet⁷⁰². Cette définition est produite pour décrire un système institutionnel complexe en constante évolution et fondé sur une approche qui se revendique multipartite et décentralisée⁷⁰³. En théorie, cette posture est sensée garantir une forme d'indépendance de la structure de tout

⁶⁹⁸ Avec notamment un important travail de Jon Postel, informaticien américain, ayant travaillé sur Internet à la fois au plan technique par la rédaction de normes et au plan institutionnel en tant que responsable de l'*Internet Assigned Numbers Authority* (IANA) division de l'ICANN chargée de l'administration des adresses IP.

⁶⁹⁹ Le dernier en date fut la 13^{ème} édition de l'Internet Governance Forum à Paris en novembre 2018.

⁷⁰⁰ Groupe de travail sur la gouvernance de l'Internet (GTGI), *Rapport du Groupe de travail sur la gouvernance de l'Internet*, juin 2005, p.3

⁷⁰¹ Sur l'importance de l'acteur privé, voir BARBAROUX Pierre, op-cit. 2014.

⁷⁰² Ibid, p.4

⁷⁰³ Voir à ce sujet notamment l'article MASSIT-FOLLEA Françoise, « Internet et les errances du multistakeholderism », *Politique étrangère*, 2014/4 (Hiver), p. 29-41. Pour une mise en perspective des problématiques soulevées dans de dernier article, voir également DELMAS Richard, « L'Internet, gouvernance d'un monde incertain », *Revue française d'administration publique*, vol. 110, no. 2, 2004, pp. 217-224 ; ainsi que MASSIT-FOLLEA Françoise, « De la régulation à la gouvernance de l'internet. Quel rôle pour les usagers-citoyens ? », *Les Cahiers du numérique*, vol. 3, no. 2, 2002, pp. 239-263.

monopole de la décision en son sein. En pratique, cela n'empêche pas la controverse. Internet tel que nous le connaissons au quotidien par le Web et les courriels est le produit de la rencontre de deux grands ensembles techniques fondamentaux : d'une part, les protocoles (IP, TCP, UDP pour les plus connus) décentralisés, et certaines infrastructures comme le Domain Name Système (DNS) qui sont très centralisés. Les serveurs racines qui gèrent les domaines de premier niveau sont au nombre de 13 dont 1 au Japon, 2 en Europe, et 9 aux États-Unis. Ces premiers serveurs sont placé sous l'autorité de l'ICANN.

Plusieurs organisations assument le volet technique de la gouvernance d'Internet : L'*Internet Society* (ISOC), association de droit américain à vocation internationale basée à Reston en Virginie, créée en 1992 par Vinton Cerf et Robert E. Kahn⁷⁰⁴ pour promouvoir et coordonner le développement des réseaux informatiques dans le monde ; et qui a notamment pour rôle de fournir un support organisationnel et financier à un autre organe de cette gouvernance : l'*Internet Engineering Task Force* (IETF) qui est une sorte de forum technique créé en 1986 et basé à Fremont en Californie, qui élabore et valide les standards Internet. L'*Internet Engineering Steering Group* (IESG) est une émanation de l'IETF qui a pour charge de coordonner l'élaboration des standards Internet. L'*Internet Architecture Board* (IAB)⁷⁰⁵ qui a pour mission de fournir une direction technique à long terme pour le développement d'Internet, garantissant qu'Internet continue de croître et d'évoluer en tant que plate-forme de communication. L'ICANN et l'IANA dont nous avons déjà parlé font également partie de cette gouvernance. Il est important ici de s'attarder sur la notion de groupe quand on parle de l'IETF ou de l'IESG. En tant que groupe, la plupart de ces organes existent de manière informelle, sans statut, sans membre, sans adhésion. Le travail technique est accompli dans une centaine de groupes de travail qui pour la plupart sont des listes de courriels. Autrement dit, la gouvernance d'Internet a ainsi pour trait caractéristique d'avoir une forte concentration de ses institutions sur le sol américain.

Néanmoins le déséquilibre est plus étendu qu'une seule question d'équilibre institutionnel. Elle touche fondamentalement au « réseau des réseaux » avec la question de l'asymétrie dans l'interconnexion d'Internet. Celle-ci suppose que chaque opérateur s'interconnecte en local, en national ou à l'international. En matière de transit, cela crée un

⁷⁰⁴ Cf. chapitre 1.

⁷⁰⁵ A l'origine, au moment de sa création par la DARPA en 1979, elle se dénommait *Internet Configuration Control Board* puis elle a changé de nom de nombreuses fois avant d'adopter cette dénomination en 1992.

système informel de trois catégories d'opérateurs répartis entre Tiers 1 (international), 2 (national) et 3 (local). La plupart des États ont accès aux Tiers 2 et 3. Ce n'est pas le cas du Tiers 1 auquel la plupart des États n'ont pas accès. En pratique le Tiers 1 est suffisamment puissant pour fixer le prix de l'interconnexion aux entreprises de moindre taille. Par ailleurs, les opérateurs de Tiers 1 ne payent pas de frais d'interconnexion entre eux. En 2017, il y avait 15 opérateurs qualifiés de Tiers 1 dont seuls 5 sont aux États-Unis. 7 sont sur le continent européen mais répartis entre divers États (France, Allemagne, Pays-Bas, Italie, Royaume-Uni, Espagne, Suède), et il y en a 3 en Asie (2 au Japon, 1 en Inde). Cette situation est particulièrement difficile pour les États en voie de développement qui n'ont pas facilement accès à ces opérateurs.

Par l'intrication des dimensions politiques, normatives, techniques et de la multiplicité d'acteurs qu'elle mobilise ainsi que des solutions qu'elle appelle, la gouvernance d'Internet est sans doute l'un des sujets les plus complexes en termes de gouvernance internationale⁷⁰⁶. Avant d'aborder la situation française, nous allons aborder un type d'acteur particulier au sein de cette gouvernance qui concerne directement la sécurité : les CSIRT.

2 – Le rôle de l'expert technique dans les relations transnationales en matière de sécurité : l'exemple des CSIRT.

Dans un article de novembre 2018⁷⁰⁷, Leonie Maria Tanczer, Irina Brass et Madeline Carr analysent les *Computer Emergency Response Team* (CERT) ou *Computer Security Incident Response Team* (CSIRT) sous l'angle de la communauté épistémique. L'approche est légèrement différente de celle que nous avons ici, mais n'en reste pas moins intéressante. Ces équipes sont composées d'experts dont la mission est de remédier aux cyberincidents. En tant que communauté d'acteurs non étatiques, ces équipes fournissent des services de sécurité essentiels et le font en grande partie à l'abri des contraintes de la gouvernance d'Internet. En tant qu'entités expertes, ces groupes agissent non pas sur la définition du vocabulaire de la sécurité mais produisent directement la sécurité elle-même. En juillet 2019, le *Forum of*

⁷⁰⁶ Nous détaillerons une partie de la réception de cet enjeu au sein des Théories des Relations Internationales dans le Chapitre 4,

⁷⁰⁷ TANCZER Leonie Maria, BRASS Irina et CARR Madeline, « CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy », *Global Policy*, vol. 9, 2018, pp. 60–66.

Incident Response and Security Teams qui est la première plateforme regroupant ce type d'acteurs dénombre 492 équipes de ce type réparties sur l'ensemble des continents.

L'étude de Tanczer, Brass et Carr est particulièrement intéressante dans la mesure où elle nuance notre relecture de la communauté épistémique. En effet, cette étude tend à démontrer que l'action collective en matière de cybersécurité transnationale est fondée sur les actions de communautés d'experts en informatique qui ont mis en place des mécanismes collaboratifs de gouvernance indépendamment des accords internationaux conclus par les États. Les « canaux de confiance » qui constituent les liens entre les différentes équipes :

« La reconnaissance de la complémentarité entre ces communautés est également importante. En collaborant autour d'un besoin technique clairement défini, les actions thématiques des CSIRT peuvent alimenter et soutenir les efforts d'autres acteurs non étatiques et étatiques en vue de résoudre l'action collective mondiale en matière de cybersécurité. Leurs pratiques ne remplacent pas ni n'occultent les autres mécanismes diplomatiques - y compris ceux mis en œuvre par des acteurs étatiques - mais elles nous aident à identifier et à comprendre les exemples subtils de diplomatie scientifique qui pourraient autrement être négligés. »⁷⁰⁸

La connaissance technique et l'objectif affiché sont suffisants pour former le socle d'influence de la communauté. Cet objectif unificateur est un élément qui indique la formation d'une communauté épistémique par les équipes malgré leurs diversifiées sur les plans géographique et sectoriel. La question de l'influence demeure posée. En effet, ces équipes ne participent directement à influencer les discussions des acteurs régaliens au sein du processus diplomatique. Mais il faut souligner ici le caractère mixte de toutes ces équipes. Lesquelles peuvent être mises en place à la fois dans les infrastructures de l'État et dans les organisations privées⁷⁰⁹. Les communautés de CSIRT constituent ainsi une interface entre l'ensemble des (grands) acteurs concernés par la sécurité de l'information.

Ce type d'acteurs mériteraient sans aucun des recherches plus avancées Malheureusement, sauf exceptions, les membres de ce type d'organisations participant assez

⁷⁰⁸ Ibid. p. 64.

⁷⁰⁹ Sur ce point et sur la coopération voir : FINNEMORE Martha, et HOLLIS Duncan B « Constructing Norms for Global Cybersecurity. » *American Journal of International Law*, vol. 110, no. 3, 2016, pp. 425–479 Ainsi que CARR Madeline, « Public–private Partnerships in National Cyber-Security Strategies » *International Affairs*, vol. 92 n°1, pp. 43–62.

peu aux évènements à caractère scientifique dans le domaine des sciences humaines. Ils n'ont ainsi pas pu faire partir du terrain de cette thèse.

Section 3 – La place du phénomène linguistique « cyber » dans les enjeux de sécurité de l'information en France.

Situer historiquement le phénomène discursif est complexe dans la mesure où cela ne revient ni à se focaliser sur l'histoire de l'enjeu de la sécurité de l'information, ni sur celle de l'artefact Internet, ni sur celle du terme « cyberspace » en particulier. Par son socle ambivalent et par les multiples intérêts dont elle est objet, la notion de « cyber » résiste aux tentatives de définition. Au-delà de l'emploi du marqueur qui reste une affaire de mode, il faut donc rechercher d'autres éléments qui permettent la définition d'une communauté. Il est impossible de se contenter de pointer du doigt une forme d'émergence *a posteriori* de la création du terme dans la science-fiction car les trois idées à la base du discours sont présentes à la base de la notion. L'enjeu serait plutôt d'identifier à partir de quelles publications le discours a cessé de concerner l'œuvre de fiction pour décrire la réalité.

Ici commence la difficulté car une œuvre de fiction, et plus généralement la production artistique, peut toujours être regardée comme une forme de discours sur le réel. La question que nous poserons ici sera donc de déterminer le moment où, par la circulation des idées, le cyberspace se met au service d'une connaissance experte propre à nourrir une forme d'influence politique. Autrement dit, à partir de quel moment le cyberspace devient-il un objet intellectuel légitime en dehors des œuvres de fiction ? C'est dans cette transition particulière que l'on peut commencer à analyser le discours comme l'un des regroupements de tendances au sein d'une communauté épistémique de la sécurité de l'information.

Cette précaution nous permet d'éviter deux pièges : d'une part, tomber dans une forme d'illusion chronologique qui reviendrait à ordonner de manière séquencées des choses qui ne le furent pas ; d'autre part, à trop nous focaliser sur une vision compatible avec l'intérêt régaliens, nous en oublierions de situer ces mêmes enjeux par rapport aux nombreuses perspectives critiques portées contre ces visions et qui participent tout autant à la production communautaire autour de la sécurité de l'information (notamment les *hackers*).

Pour contextualiser l'émergence du phénomène discursif « cyber » en France. Il faut donc bien distinguer ce phénomène de l'enjeu de la sécurité de l'information. Ce qui est

intéressant ce n'est pas de retracer l'ensemble des évolutions de l'enjeu de la sécurité de l'information. Mais de cerner le moment à partir duquel on commence à employer des cybtermots pour qualifier la sécurité de l'information.

A – Les sources du langage « cyber » : une idée anglo-saxonne en France ?

L'objectif ici est d'étudier de manière critique l'influence internationale qui produit une grande partie des définitions, notions et concepts qui sont ensuite repris dans les normes ou les travaux de recherche ou par les institutions en France qui emploie le langage « cyber ». En effet, s'il est facile, de comprendre le caractère profondément étatique de la sécurité de l'information. Les termes dans lesquelles celle-ci est conceptualisée sont pour la plupart importé. La plupart des définitions du cyberspace lorsque les États souscrivent à cette idée pour décrire les problèmes de sécurité de l'information sont le plus souvent des reprises de définitions américaines parfois améliorées et parfois telles quelles. Par ailleurs, de nombreux chercheurs issus d'institutions publiques ou privées américaines ont contribué à la définition de protocoles et de normes internationales liés à la question de la sécurité de l'information.

Il faudra néanmoins relativiser cette influence dans la mesure où elle n'est qu'une partie d'un phénomène plus vaste dans un contexte où la langue internationale pour la recherche est l'anglais et que les Relations Internationales sont fortement dépendantes des publications anglo-saxonnes pour la plus grande partie de leurs cadres théoriques. Il n'en reste pas moins que les États-Unis d'Amérique ont un rapport particulier à Internet, qu'il s'agisse de son invention, de la possession des infrastructures essentielles au fonctionnement de ses applications majeure et de sa gouvernance en général. Internet est d'une façon générale représentée comme un artefact américain depuis les années 90. Parmi toutes les langues, l'anglais a un statut particulier à l'échelle de l'informatique. Comme nous l'avons vu dans le premier chapitre, le mot cyberspace a été forgé par un auteur américain comme l'est la plupart de l'héritage scientifique et culturel qui entoure la notion.

Nous prendrons quatre exemples qui viennent illustrer cette influence : la cyberguerre, le modèles des « couches », la controverse autour de l'élaboration des *Manuels de Talinn*⁷¹⁰.

⁷¹⁰ Nous n'aborderons pas ici le texte de la déclaration d'indépendance du cyberspace de John Perry Barlow écrit tout d'abord en réponse au *Telecommunications Act of 1996* et qui s'attaque à l'applicabilité des logiques gouvernementales à la croissance du Cyberspace. L'auteur y place Internet en dehors des lois et des frontières. Il

1 – La cyberguerre ou le mythe de la révolution stratégique : la RAND Corporation.

Les études stratégiques s'appuient souvent sur la notion de révolution, les écrits des chercheurs de la RAND Corporation ne font pas exception. S'intéresser à la production de ce think tank en matière de cybersécurité est utile afin de dégager les principales sources de définitions mobilisées par la défense américaine dans ses différentes approches du cyberspace dans les années 2000 comme notion servant à définir la sécurité de l'information malgré tous les raccourcis, les imprécisions et les confusions dont elle est encore l'objet.

Avec une influence historiquement construite autour des objets de l'*air power* et des technologies de l'information, la *RAND⁷¹¹ Corporation* est un think tank international américain ayant différentes emprises en Amérique, en Europe et en Australie. Cette organisation a été créée par l'industriel américain *Douglas Aircraft Company* sous contrat avec l'*US Air force* en mai 1948 afin de conseiller l'armée et le gouvernement sur les politiques publiques à partir de recherche en analyse stratégique. En 2014, le chiffre d'affaire déclaré de cet organisme à but non-lucratif était de 351,7 millions de dollars. La « RAND » est principalement connue pour ses travaux sur les questions de défense et de sécurité mais travaille aussi sur l'économie, l'enfance, la justice, la santé, l'énergie ou encore l'environnement...⁷¹². Ce think tank a fait l'objet de plusieurs études qui ont pour trait commun de mettre en question

prône également la mise en place d'un contrat social propre à Internet autour de la Règle d'Or : L'éthique de la réciprocité. Néanmoins, même s'il est parfois cité, ce texte influent n'a eu que peu d'influence sur la communauté étudiée. Nous n'aborderons pas non plus toute la question de l'influence internationale (et pas seulement des États-Unis) au travers des puissantes compagnies des technologies de l'information Facebook, Amazon, Tencent, Google, Apple, Samsung, Baidu, Alibaba, Microsoft, IBM ou Tencent étant donné qu'elle ne traduit pas directement en influence conceptuelle du point de vue du discours. En revanche, cette chapitre étant centré sur la communauté épistémique nous réservons l'exemple de l'influence directe du Droit des États-Unis sur les autres systèmes juridiques pour le chapitre 5.

⁷¹¹ RAND est l'acronyme de "Research AND Development". Ci-après dénommée « la RAND ».

⁷¹² La *RAND Corporation* existait auparavant sous le nom de *Project RAND*, organe créé en octobre 1945 après accord du *War Department*, de l'*Office of Scientific Research and Development*, et de l'industriel. Ayant commencé ses travaux en décembre 1945, cet organe s'est notamment fait connaître par la publication d'un rapport en Mai 1946 intitulé *Preliminary Design of an Experimental World-Circling Spaceship*.

son influence sur les politiques publiques américaines (Même si cette organisation n'a pas pour seul client l'administration américaine)⁷¹³.

Le travail de conceptualisation du cyberespace en stratégie par les chercheurs de la RAND est processus assez long qui couvre une période allant de 1993 à 2007 avec de nombreuses publications. La première publication qui inaugure ce travail est le fameux article « Cyberwar Is Coming ! » de 1993 par John Arquilla et David Ronfeldt⁷¹⁴. C'est un article exceptionnel pour trois raisons principales. D'une part, cet article théorise la cyberguerre (au moins pour ce qui relève des études stratégiques). D'autre part, il est l'un des premiers à employer un terme dérivé du cyberespace pour décrire un enjeu de sécurité de l'information dans le monde réel. Et enfin, dans toute la littérature sur le cyberespace qui mobilise ce dernier pour décrire la sécurité de l'information, c'est sans doute l'un des textes le plus systématiquement cité dans les publications sur la cybersécurité toute discipline confondue. Ils sont également repris dans une partie de la « littérature grise » américaine. Ce texte a pour thème principale l'idée selon laquelle la révolution de l'information et les innovations organisationnelles connexes modifient la nature des conflits et les types de structures, doctrines et stratégies militaires nécessaires.

L'article introduit spécifiquement deux termes : la *cyberwar* et la *netwar*.

« La *Netwar* fait référence aux conflits liés à l'information à un niveau élevé entre nations ou sociétés. Cela signifie essayer de perturber, d'endommager ou de modifier ce qu'une population cible sait ou pense connaître elle-même et le monde qui l'entoure. La *Netwar* peut être axée sur l'opinion publique ou l'élite, ou les deux. Cela peut impliquer des mesures diplomatiques publiques, des campagnes de propagande et psychologiques, une subversion politique et culturelle, une supercherie ou une ingérence dans les médias

⁷¹³ Par exemple, pour les plus connues : ABELLA Alex, *Soldiers of Reason: The RAND Corporation and the Rise of the American Empire*, Mariner Books, mai 2009, 408 p. ; GHAMARI-TABRIZI Sharon, *The Worlds of Herman Kahn: The Intuitive Science of Thermonuclear War*, Harvard University Press, 2005, 432 p.; KAPLAN Fred (1983), *The Wizards of Armageddon*, Stanford University Press, août 1991, 452 p. ; SAMAAN Jean-Loup, *La RAND Corporation (1989-2009): La reconfiguration des savoirs stratégiques aux États-Unis*, Paris, l'Harmattan, 2010, 252 p.; SMITH Bruce (1966), *The RAND Corporation: Case Study of a Nonprofit Advisory Corporation*, Harvard University Press, 2013, 348 p.

⁷¹⁴ ARQUILLA John, et RONFELDT David. « Cyberwar Is Coming! » *Comparative Strategy*, vol. 12, no. 2, 1993, pp. 141–165. D'autres auteurs ont publié des textes relatifs au cyberespace à la suite de cette première étude. Il en ressort une certaine confusion autour de nombreux concepts. Ce texte fait également parti des débats sur la possibilité/probabilité d'une cyberguerre (ou non). Voir, RID Thomas, 2011 op-cit. ; voir également : STONE John, « Cyber WarWillTake Place! » *Journal of Strategic Studies*, vol. 36, no. 1, 2013, pp. 101–108. Pour la France, voir enfin, BAUD Michel, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique étrangère*, no. 2, été 2012, pp. 305-316.

locaux, une infiltration de réseaux informatiques et de bases de données, ainsi que des efforts pour promouvoir des mouvements dissidents ou d'opposition sur des réseaux informatiques. »⁷¹⁵

« La *cyberwar* se réfère à la conduite d'opérations militaires et à la préparation de celles-ci conformément aux principes relatifs à l'information. Cela signifie bouleverser, sinon détruire, les systèmes d'information et de communication, au sens large, pour inclure même la culture militaire, sur lesquels un adversaire s'appuie pour se connaître : qui est-il, où est-il, que peut-il faire quand, pourquoi il se bat, qui menace de contrer d'abord, et ainsi de suite. Cela signifie essayer de tout savoir sur un adversaire tout en l'empêchant d'en savoir plus sur lui-même. »⁷¹⁶

Ces deux concepts sont construits dans l'opposition entre l'armée et la société mais renvoient tous deux à une notion d'information assimilée à la connaissance. L'ouvrage de Jean-Loup Saaman consacré à la RAND décrit comment la *cyberwar* et la *netwar* sont parvenus à convaincre l'administration américaine de financer une étude. Il décrit un processus qui fonctionne grâce à la « reconversion de savoirs post-Guerre froide » des chercheurs, l'« interaction entre les individus » (chercheurs et militaires du pentagone) et enfin « la captation, par la RAND, des capitaux propres de ses chercheurs »⁷¹⁷. Après une série de publications diverses consacrées à l'information il ressort une grande confusion conceptuelle allant de l'*information warfare* aux *information operations* en passant par le cyberspace qui mélangeant la guerre psychologique et la guerre informatique. Cette confusion sous doute en partie due à l'administration américaine. Il faut attendre 2007 et la parution de *Conquest in Cyberspace* de Martin Libicki⁷¹⁸, pour que la multiplication des nouveaux concepts s'estompe. A l'aune de son travail sur les concepts, la question de considérer la RAND comme une pôle de la communauté épistémique se pose.

2 – Le modèle des « couches » pour décrire le cyberspace.

De nombreux textes institutionnels analysés reprennent l'idée d'un cyberspace structuré « en couches ». Cela est vrai dans la production onusienne, européenne et également

⁷¹⁵ ARQUILLA John, et RONFELDT David, 1993, op-cit. p. 144. (Notre traduction)

⁷¹⁶ Ibid. p. 146. (Notre traduction)

⁷¹⁷ L'ouvrage se base notamment sur un entretien avec David Ronfeldt. SAMAAN Jean-Loup, 2010, op-cit. pp. 113 -154.

⁷¹⁸ LIBICKI Martin C., *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press, 2007, 336 p. ; voir également LIBICKI Martin C., *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND Corporation, 2009, 144 p.

française. En 2010, l'armée américaine a proposé ce modèle en couche pour décrire le cyberespace⁷¹⁹. Selon ce modèle le cyberespace est un ensemble transversal composé de trois couches (« *layers* ») : physique, logique et sémantique.

La première couche est une couche dite matérielle (« *physical layer* »). Cette comprend tous les appareils : ordinateurs, systèmes informatiques, mais aussi si toute infrastructure d'interconnexion (câble, ondes, relais, systèmes de transmission...) ainsi que les structures de support (énergie, refroidissement des systèmes). Cette couche se divise en deux composantes : une composante géographique (localisation) et une composante physique du réseau (matériel et infrastructure). Du point de vue, de cette partie du modèle, le cyberespace n'est pas universel, il ne fait pas preuve d'ubiquité. Il est géographiquement localisé. Bien que la mobilité des utilisateurs permis par les technologies de l'information (corpus 4 et 5) permette de fluidifier sa répartition dans les zones du globe où ces technologies sont présentes.

La couche logique (« *logical layer* ») permet quant à elle d'intégrer le fameux code informatique qui recoupe tout programme, ainsi que les flux de données entre les machines, et les protocoles réseaux qui permettent cette circulation. Cette couche logique est majoritairement responsable de la transversalité, de l'opacité du cyberespace. La question de société des normes techniques et juridiques est ici fondamentale.

Enfin, la couche sémantique (« *semantic layer* » ou « *social layer* » en fonction de la source.) conceptualise la dimension informationnelle et sociale par excellence du cyber puisqu'elle recouvre tout le « sens » de l'information : le contenu ainsi que le champ des perceptions et représentations. Dans sa conception sociale, cette couche se détache du contenu et intègre principalement les composantes de « persona » (assimilables en pratique aux acteurs d'un réseau) et de « cyber persona » (principalement relatives aux données personnelles des utilisateurs).

Force est de constater que ce modèle a connu un certain succès dans les descriptions du cyberespace. Ou du moins que cette représentation peut être mobilisées par les chercheurs pour circonscrire la question de la technique : Le modèle est présent dans la plupart des essais et des livres scientifiques publiés en France depuis 2010. Ce modèle permet de discriminer les

⁷¹⁹ *Cyberspace opérations concept capability plan 2016-2018, TRADOC Pamphlet 525-7-8*, Fort Monroe, États-Unis, 22 février 2010. (Sur ce point voir en particulier le chapitre 2 du document pp. 8 – 14).

politiques en fonction de leur nature technique. Par exemple, la protection des données personnelles aurait a priori trait aux couches sémantique et logiques plutôt qu'à la couche matérielle. La « fracture numérique » entre États ayant accès à Internet ou non relèvera prioritairement de la couche matérielle. Le débat autour de la « neutralité du net »⁷²⁰ sera avant tout un problème de la couche logique. Ces couches sont également considérées différemment selon les différents États. Plus précisément, elles permettraient ainsi que catégoriser les différents États en fonction des relations qu'ils entretiennent avec chacune de ces dimensions. Une tendance générale assez caricaturale de la réalité veut que l'Europe et les États-Unis soient davantage portés sur les deux premières couches, tandis que Chine et Russie seraient davantage porté sur les couches logique et sémantique. En pratique, il est difficile de dire qu'un État « se focalise » sur telle ou telle couche alors que chaque État par un discours totalement différent.

De plus comme nous l'avons vu, certains États comme la Russie, n'utilisent pas l'expression « cyberspace » ou les termes dérivés. Toutefois, si ce modèle a le mérite de réunir la plupart des ingrédients dans un modèle cohérent elle ne permet pas de traduire l'ensemble de l'impact du langage « cyber » qui est constitué principalement non pas d'un corpus technologique mais par le pouvoir évocateur. Tout juste, cette représentation n'est qu'une traduction de l'artefact Internet dans une logique de granularité technocentrée mais dont le contenu évolue sans cesse. Ainsi les structures de support (énergie, refroidissement des systèmes) ne sont pas présentes dans le modèle et ne sont intégrée qu'après. De même pour les smartphones et les autres systèmes intelligents, puis l'Intelligence Artificielle qui viendra s'ajouter au modèle dans la plupart des conférences. A l'inverse, les dimensions électronique et électromagnétique présentes dans la publication américaine originaire ne sont pas reprises.

3 – La controverse autour de l'élaboration des *Manuels de Tallinn*.

Suite aux événements estoniens de 2007, l'OTAN a ordonné la création d'un centre d'excellence dédié à la cyberdéfense à Tallinn⁷²¹. Ce centre a servi de structure de support aux deux versions du projet de « Manuel de Tallinn ». Il s'agit d'une étude universitaire non contraignante sur l'application du droit international aux cyberconflits et à la cyberguerre élaboré entre 2009 et 2012. La première version intitulée *Tallinn Manual On The International*

⁷²⁰ Le principe qui dispose l'égalité de traitement de tous les flux de données sur Internet.

⁷²¹ NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) créé le 14 mai 2008.

Law Applicable To Cyber Warfare a été publiée en février 2013⁷²². Tandis que la seconde *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* a été publiée en février 2017⁷²³. En tant que document non-constraining, ce document n'incarne que la vision de ses auteurs et non pas l'OTAN ou à fortiori des États membres de cette alliance⁷²⁴. C'est donc deux documents de « doctrine » au sens juridique du terme. La première version de ce manuel est parvenu sur la base du consensus à mettre en place 95 règles de Droit. Ce sont des textes assez exceptionnels en Droit International public.

Le groupe mandaté par l'OTAN pour concevoir cet ouvrage était dirigé par Michael Schmitt, directeur du département de droit international au Naval War College (États-Unis), avec 19 autres personnalités issus des mondes de la recherche et des armées en provenance des États-Unis, du Canada, du Royaume-Uni, d'Allemagne, de Suisse, des Pays-Bas et de l'Australie⁷²⁵. Au-delà des choix des manuels ou de leur principe⁷²⁶, la critique majeure adressée à ces travaux tenait en effet de la composition du groupe d'experts regroupant majoritairement des anglo-saxons, ce qui des questions de représentativité et d'objectivité. Le groupe a été modifié pour la version 2.0 en intégrant notamment quelques experts asiatiques sans que cela ne fasse vraiment taire les critiques.

Du point de vue de cette recherche, ce manuel constitue un outil de légitimation de l'enjeu de la sécurité de l'information comme enjeu de sécurité nationale. En opérant la traduction de la notion de cyberguerre, cyberattaque ou cyberopération dans le cadre du droit de faire la guerre (*jus ad bellum*) et du droit dans la guerre (*jus in bello*) tout en ayant une position tournée vers le droit tel qu'il existe (*lex lata*) plutôt que sur un droit à créer (*lex*

⁷²² SCHMITT Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013, 304 p

⁷²³ SCHMITT Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017, 638 p.

⁷²⁴ Pour rappel, une position de l'OTAN est toujours prise sur la base du consensus et représente la volonté de tous les membres de cette alliance militaire et politique.

⁷²⁵ Outre les 20 personnalités, l'OTAN était représentée dans le projet par le Commandement Allié de la Transformation, étaient également représenté le Comité international de la Croix-Rouge ainsi que le *United States Cyber Command*. Par ailleurs, le

⁷²⁶ Considérant les législations et le droit informatique de chacun des États mobilisés dans le dispositif et les normes techniques internationales dédiées à l'informatique, la question de la bonne norme juridique internationale se pose techniquement un peu moins que celle de l'application et de l'efficacité de la norme existante notamment au travers de l'enjeu de « l'attribution » des cyber-attaques.

ferenda)⁷²⁷, les auteurs participent de la consécration de l’enjeu de sécurité et de sa légitimation comme objet de sécurité d’un État. En tant que producteurs de discours savants raisonnant sur la base du consensus dans une perspective de définition des termes, nous avons ici une forme de projet informel qui correspond aux définitions de la communauté épistémique « classique » et semble représenter un bon pôle de celle sur la sécurité de l’information dans la perspective que nous avons adoptée ici.

B – L’émergence de la sécurité de l’information avant la mode du Cyberespace en France.

Dans la littérature sur la cybersécurité, il existe beaucoup de références à la cryptographie ou aux services secrets de l’antiquité jusqu’aux Guerres mondiales. Nul doute que l’information est un enjeu de sécurité depuis longtemps. Cependant, notre discours fonctionne avec une modalité particulière de la sécurité de l’information qui réside dans le fait que cette information est automatisée, numérique... La question à se poser n’est plus de savoir quand l’information est-elle devenue un enjeu de sécurité ? Mais quand l’informatique est-elle devenue un enjeu de sécurité ? Et plus spécifiquement quand est-ce que les États et notamment la France ont décidé la considérer comme telle ?

Nous distinguerons ici deux temps en abordant d’une part, aux origines de la sécurité informatique dans la littérature de l’État français (c’est-à-dire depuis l’introduction de l’outil informatique) et d’autre part, seront examinées les premières publications en français à mélanger l’intérêt régional, sécurité de l’information et intérêts étatiques. Ce qui nous entraînera donc des années 60-70 jusque dans les années 90.

1 – Les origines de l’informatique et de la sécurité informatique en France.

Le moment important de la transformation enjeu de sécurité de l’informatique réside dans la transition entre la mécanographie et l’informatique dans l’administration publiques entre les années 60 et les années 70⁷²⁸. L’informatique va peu à peu devenir le terrain de tous

⁷²⁷ Quand bien même, la présence des Manuels n’écarte pas la possibilité de nouvelles normes.

⁷²⁸ Sur le sujet de la transition entre la mécanographie et l’informatique, voir en particulier pour l’exemple français la synthèse fournie par le rapport post-doctoral, BAUDOT Pierre-Yves, *La compatibilité des systèmes. L’informatique dans le jeu administratif: Préfectures, Collectivités Locales et ministère de l’Intérieur, 1966-1975*, Rapport de post-doctorat, UMR CNRS 5206 Triangle, juin 2007, 95 p. Voir également, BAUDOT Pierre-

les débats antérieurs sur la mécanographie utilisée dans l'administration française depuis les années 30, notamment au Ministère des finances. Aux lendemains de la Deuxième guerre mondiale, le nouvel Institut de la statistique et des études économiques (INSEE) créé le 27 avril 1946, se voit confier le traitement des données du ministère mais perdra peu à peu le monopole de cette mission au profit d'autres ateliers de statistique⁷²⁹.

Suite à quelques initiatives isolées au sein de l'administration, une circulaire du Premier ministre Georges Pompidou adressée le 7 décembre 1967 aux ministres et secrétaires d'État demande le remplacement des commissions de mécanographie au profit de nouvelles commissions dédiées à l'informatisation des ministères⁷³⁰. Le 15 janvier 1968, le Ministère de l'Intérieur crée sa nouvelle commission qui va rapidement se retrouver chargée de piloter l'informatisation des services centraux, des services déconcentrés, des départements et des communes.

En parallèle de ce processus, l'information en tant qu'objet devient peu à peu l'un des indicateurs des bonnes relations entre les administrations et entre les administrations et les administrés⁷³¹. En tant que tel, l'informatique semble donc un outil idéal pour accompagner la réforme de l'administration, notamment pour lui permettre de centraliser l'information administrative, économique et sociale dans les préfectures⁷³². Cette centralisation correspond dans l'esprit à l'intégration complète des circuits d'information et une prise de décision automatisée. L'informatique est présentée en tant que technologie de gouvernement qui rompt avec la répartition des tâches antérieures au sein de l'administration.

« Portée par les informaticiens, cette représentation de l'informatique comme rupture renforce donc l'importance symbolique des ressources financières dont les conseils généraux disposent pour s'équiper en informatique. Plus surprenant : bien qu'elle prive partiellement l'État central du contrôle de la collecte

Yves. « L'incertitude des instruments. L'informatique administrative et le changement dans l'action publique (1966-1975) », *Revue française de science politique*, vol. vol. 61, no. 1, 2011, pp. 79-103. Pour une synthèse l'évolution de l'informatique dans l'administration de façon plus générale et notamment l'introduction de la micro-informatique dans les périodes suivantes (1978-1995), voir DAGIRAL Éric. « Administration Électronique. » *Communications*, vol. 88, no. 1, 2011, pp. 9-17.

⁷²⁹ FIALAIRE Jacques. « L'évolution des politiques d'informatisation de l'administration publique en France. Quelles articulations entre services centraux et déconcentrés de l'État ? » *Politiques et management public*, vol. 10, n° 4, 1992. pp. 55-63.

⁷³⁰ BAUDOT Pierre-Yves, 2011, pp. 83-84.

⁷³¹ GEOGHEGAN, Bernard., 2008, op-cit.

⁷³² Ce qui était déjà un souhait avec la mécanographie dans les années 60.

et du traitement des informations relatives à l'action de la puissance publique, cette représentation en rupture de l'instrument est également soutenue par le ministère de l'Intérieur. »⁷³³

Au-delà des effets organisationnels d'une telle réforme de l'État, il faut s'interroger ici sur la place particulière accordée à la sécurité. L'un des débats principaux autour de la sécurité et l'introduction de l'informatique dans l'administration concerne la protection des utilisateurs de l'informatique. Toutefois, l'enjeu n'est pas présent dans cette réforme particulière. Certes, l'objectif de défense des utilisateurs face aux fournisseurs est intégré dans certaines commissions informatiques s'agissant surtout de conseiller les collectivités en termes d'achat⁷³⁴. En réalité la sécurisation est le fruit de plusieurs phénomènes concomitants concernant les libertés individuelles, les fichiers policiers, l'utilisation de l'informatique dans la défense⁷³⁵.

Du côté des libertés publiques, en 1974, est révélé le projet de « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus » (SAFARI)⁷³⁶. La révélation de ce projet lance un débat important sur les libertés individuelles et l'informatique. La perspective d'un fichier unique dans l'administration pose de nombreuses questions quant au respect de la vie privée⁷³⁷. Le débat est notamment réputé aboutir à la création de la Commission nationale de l'informatique et des libertés (CNIL) par la Loi n°78-17 du 6 janvier 1978. Cette dernière loi est l'une des bases du Droit de l'informatique en France. Son article premier contient un attendu de principe qui définit une place particulière de l'informatique :

⁷³³ BAUDOT Pierre-Yves, 2011, op-cit. p. 87

⁷³⁴ Cf. la Commission Spécialisée des Marchés d'Informatique (CSMI) instituée par le Décret n°72.199 du 13 mars 1972.

⁷³⁵ Sur la question de la défense d'un point de vue global durant cette période de temps, voir BELLAIS Renaud. « Les enjeux de la maîtrise de l'information dans la défense. » *Réseaux*, volume 16, n°91, 1998. Les relations clients-fournisseurs à l'épreuve des réseaux. pp. 121-133. Voir également l'ouvrage WARUSFEL, Bertrand. *Contre-Espionnage Et Protection Du Secret: Histoire, Droit Et Organisation De La sécurité Nationale En France*. Parisn Lavauzelle, 2000, 496 p.

⁷³⁶ Projet lancé en 1973 qui consistait à regrouper toutes les fiches de l'administration en un seul fichier qui regrouperait environ 400 fichiers des services de police ainsi que des ministères de la justice, des armées, la sécurité sociale, les banques. Voir, BOUCHER Philippe, « Safari ou la chasse aux français », *Le Monde*, 21 mars 1974, p. 9. Cette affaire n'était d'ailleurs pas la seule puisqu'elle suivait l'affaire dite « des plombiers », ou « watergaffe » du 3 décembre 1973 impliquant la pose de mouchards dans les locaux du Canard enchaîné par des personnels de la Direction de la Surveillance du territoire.

⁷³⁷ Voir l'ouvrage GALLOUEDEC-GENUYS Françoise, et MAISI Herbert, *Le Secret Des Fichiers*, Éditions Cujas, 1976, 328 p. Ainsi que ROBERT Pascal, *L'impensé informatique: critique du mode d'existence idéologique des technologies de l'information et de la communication*, Volume 1, Archives contemporaines, 2012, 234 pages.

« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »⁷³⁸

Durant l'ensemble de la période considérée, les moyens de cryptologie, publics comme privés, sont toujours soumis au statut de 1939 et à l'assimilation à des matériels de guerre⁷³⁹. Tout moyen de cryptage fait donc l'objet d'une procédure de dérogation pour être employé en dehors du cadre militaire notamment dans les entreprises. L'introduction de l'outil informatique ne change pas le principe de ce dispositif. De plus les institutions chargées de la protection de l'information se suivent : Direction technique des chiffres (DTC), créée en 1943 à Alger ; Service central technique des chiffres (STC-CH), lequel lui a succédé à Paris en 1951 et qui est ensuite devenu le Service central du chiffre et de la sécurité des télécommunications (SCCST), créé en 1977⁷⁴⁰.

Dans les mêmes temps, en 1975, paraît une instruction interministérielle du Secrétariat général de la défense nationale (SGDN) qui a pour objet d'assurer la protection des informations de l'Organisation du Traité de l'Atlantique Nord, dans le cadre de la réglementation française⁷⁴¹. Elle comprend un article 29 spécifiquement dédié à la sécurité informatique afin notamment de pallier aux « défaillance des matériels et des risques d'interception, d'altération ou de destruction des données ».

A cette époque lorsqu'on parle de « cyber » au-delà de la cybernétique, c'est surtout pour désigner des calculateurs de la gamme « cyber » commercialisés par la société américaine Control Data Corporation à partir de 1974. Toutefois, les enjeux de sécurité individuelle et nationale sont déjà associés à l'information avant l'informatique. Au-delà d'un retard de l'administration par rapport aux entreprises sur le secteur, il est possible d'affirmer que cette période aboutit à une forme de diffusion de l'outil informatique dans l'ensemble des domaines de l'administration jusque dans la manière d'y organiser le travail.

⁷³⁸ Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Article 1^{er}.

⁷³⁹ Pour le statut général : *Décret-loi* du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions. Il fut modifié par le *Décret* n°73-364 du 12 mars 1973 puis par *Décret* n°86-250 du 18 février 1986.

⁷⁴⁰ L'équivalent actuel de ces services est l'Agence nationale de la sécurité des systèmes d'information (ANSSI) créée par le décret n°2009-834 du 7 juillet 2009.

⁷⁴¹ *Instruction interministérielle* n°2100/SGDN/SSD du 1^{er} décembre 1975. Cette instruction remplace alors *L'instruction générale interministérielle* n° 100/DN/ ANS du 16 janvier 1962.

2 – Les premières publications en français associant sécurité de l'information, cyber et État.

Il est particulièrement compliqué d'identifier un usage des termes en « cyber » avant la lettre en dehors de l'usage des noms d'ordinateurs que nous avons déjà évoqués. Quand bien même les termes sont déjà très répandus en anglais dans les années 80. Dès 1985, le concept de *Computer crime* laisse parfois la place à la notion de *Cybercrime* dans les recherches anglosaxonne⁷⁴².

Dans les années 90, La France quitte peu à peu le Minitel pour Internet auquel elle s'est connectée officiellement en 1988⁷⁴³. On peut en déduire que la transition du langage « cyber » vers la sécurité est à rechercher dans cette période-là. Pour des ouvrages qui mobilisent le cyberspace comme mot dans le corps du texte dans les années 90. Il faut par exemple se tourner vers des ouvrages comme celui de Joël de Rosnay⁷⁴⁴. Toutefois, malgré l'intérêt de ce type de travaux aucune association n'est faite à l'idée de sécurité. C'est en partie la raison pour laquelle, il est compliqué de mobiliser des œuvres de cette époque.

L'une des premières publications françaises que l'on peut associer au développement du discours « cyber » repose sur l'idée d'une comparaison France/États-Unis. Il s'agit de l'ouvrage *Guerres dans le cyberspace, services secrets et Internet*, écrit par le journaliste Jean Guisnel et paru en 1995 aux Éditions La Découverte⁷⁴⁵. L'un des points d'intérêt de l'ouvrage de Jean Guisnel est de présenter comment l'informatique et la cryptographie participent de l'affaiblissement de la distinction entre l'ordre interne et l'ordre international aux États-Unis.

⁷⁴² JOHNSON Deborah G *Computer ethics*. Prentice-Hall, Englewood Cliffs, 1985, 110 p.

⁷⁴³ GONZALEZ Antonio et JOUVE Emmanuelle, « Minitel : histoire du réseau télématique français », *Flux*, vol. 47, no. 1, 2002, pp. 84-89.

⁷⁴⁴ ROSNAY (DE) Joël, *L'homme symbiotique : regards sur le troisième millénaire*, Paris, Seuil, 1995, 349 p. Pour une analyse plus détaillée de cet ouvrage, voir MUSSO Pierre, 2000 op-cit.

⁷⁴⁵ GUISEL Jean, *Guerres dans le cyberspace, services secrets et Internet*, Paris, La découverte, coll. « Enquêtes », octobre 1995, 252 p.. Deux autres éditions de l'ouvrage existent en poche en 1997 et une réédition 2013 laquelle se dote d'une intéressante postface de l'auteur sur l'actualité de son enquête. Notre recherche mobilise exclusivement la première édition.

Notamment, comment les agences de renseignements légitiment par la sécurité intérieure le fait de construire et d'exercer une surveillance à l'extérieur des frontières⁷⁴⁶.

Cette tendance à la comparaison France / États-Unis dépasse la seule question de cet ouvrage si on examine quelques publications phares de l'époque qui concerne l'information. En France en 1995, les autres ouvrages français présentent l'expérience américaine comme source d'inspiration⁷⁴⁷. L'un des autres ouvrages a été écrit par un polytechnicien français Christian Huitema, membre de l'Internet Architecture Board de 1991 à 1996 et premier président non-américain de celui-ci entre avril 1993 et juillet 1995, établit la même comparaison sur des questions différentes de celles de la sécurité⁷⁴⁸. Dans un même sens, un dernier livre intéressant à l'époque en France est la version française de l'ouvrage *Being Digital (L'homme numérique)* de Nicholas Negroponte⁷⁴⁹. Toutefois ces ouvrages (y compris celui de Jean Guisnel) ne font que peu référence à la notion de cyberspace dans leur contenu ou mobilisent peu de termes dérivés de celui-ci.

Il y a plusieurs rapports officiels qui sont traditionnellement cités lorsqu'il s'agit d'aborder la question de la sécurité de l'information et d'Internet. Le premier est le rapport au Premier Ministre de Gérard Théry sur les autoroutes de l'information en 1994⁷⁵⁰. Lequel aborde notamment la sécurité des réseaux (avec plusieurs cas particuliers notamment le réseau Rénater), mais aussi la sécurité dans le cadre du développement de la domotique. Le deuxième est le rapport de Thierry Breton sur la question des téléservices de la même année⁷⁵¹. Ce rapport traite notamment de la sécurisation des échanges⁷⁵² ainsi que de divers outils de chiffrement et

⁷⁴⁶ Au cours de notre recherche, les différentes rencontres avec des chercheurs et des membres des institutions des États-Unis ou des personnes qui travaillaient sur cette question ont mis en lumière une intériorisation forte de ce type de logique.

⁷⁴⁷ A ce sujet, nous passerons également en 1995 sur la publication de la traduction de l'ouvrage de Bill Gates, *La Route du futur*.

⁷⁴⁸ HUIEMA Christian, *Et Dieu créa l'Internet*, Paris, Eyrolles, 1995, 201 p.

⁷⁴⁹ Pour la version française, NEGROPONTE Nicholas, *L'homme numérique*, Paris, Robert Laffont, avril 1995, 290 p. S'il en était encore besoin la version française du titre montre une nouvelle fois la porosité et les confusions possibles entre les concepts.

⁷⁵⁰ THERY Gérard, *Les autoroute de l'information*, rapport au Premier Ministre, Paris, La Documentation française, Janvier 1994, 98 p.

⁷⁵¹ BRETON Thierry, *Les Téléservices en France. Quels marchés pour les autoroutes de l'information ?*, rapport au ministre de l'Intérieur et de l'Aménagement du territoire, et au ministre des Entreprises et du Développement économique, Paris, La Documentation française, 1994, 615 p.

⁷⁵² Ibid. p. 41.

de télésurveillance. Le troisième est le rapport Miléo de 1996⁷⁵³ qui aborde principalement le thème de la sécurité sous l'angle des réseaux. Enfin est souvent cité également le rapport de Patrice Martin-Lalande de 1997 consacré à Internet⁷⁵⁴ qui consacre une grande partie de ses développements aux questions de sécurité. Sur tous ces documents, seul le dernier emploie le langage « cyber » en trois occurrences afin de parler non pas de sécurité mais d'accès à l'information dans le cadre de l'école à l'heure numérique et de l'accès aux données administratives dans les chambres de commerce et d'industrie⁷⁵⁵.

Pour trouver des rapports qui associent le cyberspace à la sécurité, il faut plutôt regarder du côté du juridique. En particulier ici, le rapport de 1997 au ministre délégué à la Poste aux Télécommunications et à l'Espace et au ministre de la Culture dans le cadre de la mission interministérielle sur l'Internet⁷⁵⁶. Au-delà du cybercafé ou du cybernotaire, on y retrouve le cybergendarme, la *cyberpatrol*, le cyberspace ou encore le cyberjuge...

Deux passages semblent intéressants concernant l'intérêt de l'emploi des termes « cyber » pour qualifier des enjeux de sécurité. Tout d'abord, on trouve un passage sur l'intérêt de normer le cyberspace notamment vis-à-vis de sa remise en cause des bases territoriales de l'application du Droit :

« Le cyber espace ne pourra réellement s'organiser et définir des règles communes de fonctionnement et de valeurs qu'à travers une négociation internationale sur l'édition électronique souhaitée au demeurant par la plupart des acteurs privés. Une telle négociation doit se traduire à la fois par une entraide judiciaire accrue et par l'adoption de principes communs non pas tant sur les contenus que sur la méthodologie de traitement des questions, notamment les questions de responsabilité et de loi applicable. »⁷⁵⁷

Ainsi si que, sur la gendarmerie :

⁷⁵³ MILEO Thierry (dir.), *Les réseaux de la société de l'information*, Rapport du commissariat général du plan, Groupe de travail Réseaux de la société de l'information, Paris, La Documentation française, 1996, 230 p.

⁷⁵⁴ MARTIN-LALANDE Patrice, *L'Internet : un vrai défi pour la France*, rapport au Premier Ministre, Paris, La Documentation française, 1997, 89 p.

⁷⁵⁵ Pour les écoles, l'installation de bornes Internet et de lieux labellisés « Cyberjeunes » (Ibid. p. 18). Pour les entreprises, le rapport fait référence aux « cyber- espace » des chambres de commerce et d'industrie (l'espace et le tiret sont tels quels dans le texte, Ibid. p. 24).

⁷⁵⁶ La mission s'est déroulée entre le 16 mars 1996 et le 16 juin 1996. GAUTRAUD Nathalie et FALQUE-PIERROTIN Isabelle, *Internet: Enjeux Juridiques*. Rapport au ministre délégué à la Poste aux Télécommunications et à l'Espace et au ministre de la Culture, Paris, La Documentation Française, 1997.

⁷⁵⁷ Ibid. p.

« En revanche, la création de forces d'enquête spécialisées (cybergendarmes) apparaît souhaitable pour garantir une intervention rapide et efficace contre toute forme de délinquance sur le réseau. »⁷⁵⁸

En 1998, le Conseil d'État publiait son étude sur Internet et les réseaux numériques qui prévoit notamment la lutte contre la criminalité en associant celle-ci au cyberespace, néanmoins le rapport mobilise la notion de criminalité informatique plutôt que de cybercriminalité⁷⁵⁹. L'idée reçue veut que souvent que les problématiques de l'Internet et de son rapport à la loi sont nouvelles. Le cyberespace a gagné en popularité sur cette idée reçue. Toutefois, Internet avait les mêmes enjeux politiques dans les années 90. Voici quelques mots de la synthèse de ce rapport qui viennent remettre en cause cette prétendue nouveauté :

« Internet et les réseaux numériques, c'est avant tout un nouvel espace d'expression humaine, un espace international qui transcende les frontières, un espace décentralisé qu'aucun opérateur ni aucun État ne maîtrise entièrement, un espace hétérogène où chacun peut agir, s'exprimer et travailler, un espace épris de liberté. Cet espace n'est pas naturellement celui du droit. Celui-ci, d'application territoriale, s'appuie sur des comportements, des catégories homogènes et stables, tous éléments qui font défaut dans le cas d'Internet. Cet antagonisme avec le droit aurait même, selon certains, favorisé l'essor initial du réseau, libre de toutes contraintes hormis celles fixées par la communauté des chercheurs qui sont à l'origine de sa création. Cette situation ne peut cependant plus perdurer. Le succès et la généralisation progressive d'Internet, qui est désormais un espace grand public et marchand reliant plus de 100 millions d'utilisateurs, conduit à s'interroger sur la fixation des règles de cet espace : qui les fixe, selon quelles modalités et avec quelle efficacité ? Les réponses ne peuvent plus seulement être celles d'un petit nombre de spécialistes. Elles doivent être discutées entre l'ensemble des acteurs publics et privés et faire l'objet d'un débat démocratique. »⁷⁶⁰

Ainsi dans les 90, non seulement le discours « sécurité de l'information, cyber et État » existe. Mais tous les éléments qui retrouvent aujourd'hui dans les débats existaient bien avant que le langage « cyber » ne devienne à la mode.

⁷⁵⁸ Ibid. p. 70

⁷⁵⁹ Conseil d'État, *Internet et les réseaux numériques*, Paris, La documentation française, 1998, 193 p.

⁷⁶⁰ Ibid. p. 6-7. Cette citation est notamment mobilisée dans mes cours consacrés à la question de la cybersécurité afin de faire prendre conscience aux apprenants de l'illusion de la nouveauté qui est liée à la sécurité de l'information.

C – La transformation de la sécurité de l'information en enjeux de sécurité nationale.

Après avoir analysé les débuts de la sécurité informatique et le début du discours « Cyber – Sécurité de l'information – État ». Il nous faut venir au point du tournant sécuritaire du cyberspace. Ce tournant intervient lorsque cyberspace et sécurité de l'information passe du statut de sujet de société à enjeux de la sécurité nationale.

Nous évoquerons d'une part, la consécration par le livre blanc de 2008. Et d'autre part, quelques usages antérieurs dans l'administration afin de dater l'emploi des cybarmots.

1 – Consécration de la sécurité de l'information par le Livre blanc de 2008.

La pierre angulaire de cette transformation du cyberspace en enjeux de sécurité nationale en France est le *livre blanc sur la défense et la sécurité nationale de 2008*. Lequel indique notamment :

« Les moyens d'information et de communication sont devenus les systèmes nerveux de nos sociétés sans lesquels elles ne peuvent plus fonctionner. Or le « cyberspace », constitué par le maillage de l'ensemble des réseaux, est radicalement différent de l'espace physique : sans frontière, évolutif, anonyme, l'identification certaine d'un agresseur y est délicate. La menace est multiforme : blocage malveillant, destruction matérielle (par exemple, de satellites ou d'infrastructures de réseau névralgiques), neutralisation informatique, vol ou altération de données, voire prise de contrôle d'un dispositif à des fins hostiles »⁷⁶¹

Avant d'ajouter sur la même page :

« En outre, dans la mesure où le cyberspace est devenu un nouveau champ d'action dans lequel se déroulent déjà des opérations militaires, la France devra développer une capacité de lutte dans cet espace. Des règles d'engagement appropriées, tenant compte des considérations juridiques liées à ce nouveau milieu, devront être élaborées. »⁷⁶²

⁷⁶¹ *Défense et sécurité nationale : Le Livre Blanc*, Paris, La Documentation française, 2008, p. 53.

⁷⁶² Ibid.

Cette consécration est perçue la conséquence directe des réactions après les évènements estoniens d'avril 2007⁷⁶³. Les idées d'un espace fluide et de la menace multiforme s'y retrouvent. La seconde définition ne précise pas que la lutte sera dans un premier temps exclusivement défensif.

Elle aussi un moyen pour la France de donner suite au communiqué des ministres de la défense lors de la réunion de l'OTAN à Bruxelles le 14 juin 2007. Lequel promettait une action immédiate de la part des États membres de l'alliance. Il est important de rappeler ici que ce n'est pas une affaire isolée puisque les 13 DNS ont fait l'objet d'une attaque informatique deux mois auparavant en février 2007.

2 – Le langage « cyber » et la sécurité dans les textes antérieurs à 2008.

Avant les évènements estoniens de 2007, au moment de la parution du rapport parlementaire français rédigé pat le député Pierre Lasbordes en 2006⁷⁶⁴, le langage « cyber » est déjà fortement riche et utilisé. Par exemple, il est par exemple possible d'y trouver « cyber-attaque »⁷⁶⁵, « cyber-criminalité »⁷⁶⁶, « cyber-policiers »⁷⁶⁷, « cyber-espions, cyber-terroristes et cyber-escrocs »⁷⁶⁸, « cyberspace »⁷⁶⁹, « cybersécurité »⁷⁷⁰...

Tout l'appareil discursif y est déjà présent avec une légère préférence pour le vocabulaire qui entoure la cybercriminalité. Ce n'est toutefois pas illogique : à partir de novembre 2001 s'est ouverte procédure de signature la Convention de Budapest sur la cybercriminalité que la France a ratifiée en 2003⁷⁷¹. La notion de cybercriminalité était sensée

⁷⁶³ Cf. introduction.

⁷⁶⁴ LASBORDES Pierre, *La sécurité des systèmes d'information : un enjeu majeur pour la France*, Paris, La Documentation française, Collection des rapports officiels, janvier 2006, 195 p.

⁷⁶⁵ Ibid. p. 10

⁷⁶⁶ Ibid. p. 15, et sans trait d'union : p. 49 p. 50 (deux fois), p. 56, p. 64, p. 70 et p. 71

⁷⁶⁷ Ibid. p. 30

⁷⁶⁸ Ibid p. 30 également.

⁷⁶⁹ Ibid p. 64 (trois fois dont une fois en français), p. 65,

⁷⁷⁰ Ibid p.64 (trois fois dont une fois en anglais), p. 70, p. 72, p. 74.

⁷⁷¹ Traité hébergé dans le cadre du conseil de l'Europe, référence : STE n°185. Cette convention est entrée en vigueur le 1er janvier 2007. *Loi n° 2005-493* du 19 mai 2005 autorisant l'approbation de la convention sur la cybercriminalité et du protocole additionnel à cette convention, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Voir à ce sujet l'article : CHILSTEIN David.

y recouvrir tout ce qui concernait les crimes informatiques. Néanmoins l'expression n'était présente que dans les titres et le préambule du traité et ne figurait pas du tout dans les différentes dispositions techniques.

Les premiers textes officiels de niveau étatique publiés en France à intégrer la notion de « cybercriminalité » sont des questions parlementaires. La première question est une question écrite de M. Alain Pluchet (sénateur RPR de l'Eure)⁷⁷². La question est adressée au Ministère de la justice et concerne les problèmes de pédophilie, de drogue et de tout autre commerce de médicaments illicites et dangereux dont l'obtention a été facilitée par l'existence des réseaux Internet. La réponse du ministère de la Justice publiée en 1998 intègre la phrase suivante.

« Sur le plan international, un sommet consacré à la cybercriminalité a réuni les ministres de la justice des pays du G7/P8 le 10 décembre 1997 à Washington. »⁷⁷³

Du côté de la cyberdéfense, si elle traditionnellement attribué au rapport d'information Romani de 2008⁷⁷⁴. Elle est en réalité à rechercher en novembre 2007 du côté de l'Audition de M. Michel Miraillet, directeur chargé des affaires stratégiques au ministère de la défense, le Jeudi 8 novembre 2007 devant la commission parlementaire des affaires étrangères, de la défense et des forces armées.

« M. Michel Miraillet a répondu que les attaques opérées contre les systèmes informatiques du gouvernement estonien, il y a quelques mois, avaient souligné l'actualité de la cyberdéfense⁷⁷⁵. Il a précisé que le ministère de la défense, comme tous les ministères, assurait la protection de son réseau informatique, la coordination interministérielle étant du ressort de la Direction centrale de la sécurité des systèmes d'information (DCSSI) placée auprès du Secrétariat général de la défense nationale (SGDN). Il a cité quelques exemples du rôle de veille et de protection assuré par ce service. Il a ajouté que des

⁷⁷² « Législation sur la cybercriminalité en France », *Revue internationale de droit comparé*, Vol. 62 N°2, 2010. pp. 553-606.

⁷⁷³ Question écrite n° 03127 publiée dans le JO Sénat du 02/10/1997. Réponse publiée dans le JO Sénat du 26/02/1998.

⁷⁷⁴ ROMANI Roger, *Rapport d'information* fait au nom de la commission des affaires étrangères, de la défense et des forces armées, n° 449,

coopérations étroites étaient nouées avec des pays européens comme avec des pays extra-européens tels que Singapour, ainsi qu'avec le centre de cyberdéfense de l'OTAN. »⁷⁷⁵

Il y aurait presque 10 ans entre l'introduction factuelle de la cybercriminalité dans les discours officiels d'un niveau étatique et celle de la cyberdéfense. Ce qui dénote une sécurité qui se construit d'abord sur l'idée de cybercrime avant celle de cyberguerre ou de cyberdéfense.

La cybersécurité, quant-à-elle, se développerait un peu au même moment que la cyberdéfense. Exception faite des actes du Colloque organisé par la Commission Nationale de l'Informatique et des libertés (CNIL) et l'université Panthéon-Assas-Paris II au Sénat les 7 et 8 novembre 2005 où la cybersécurité est mentionnée au titre du projet « programme mondial cybersécurité » de l'Union International des Télécommunication ainsi que de la « culture de la cybersécurité » souhaitée lors du sommet mondial sur la société de l'information de 2003 :

« [...] Une culture globale de la cybersécurité doit être encouragée, développée et mise en oeuvre en coopération avec tous les partenaires et tous les organismes internationaux compétents. [...] Dans cette culture mondiale de la cybersécurité, il importe d'accroître la sécurité et d'assurer la protection des données et de la vie privée, tout en améliorant l'accès et les échanges commerciaux. Cette culture mondiale de la cybersécurité doit en outre tenir compte du niveau de développement socio-économique des pays et respecter les aspects de la société de l'information qui sont orientées vers le développement. »⁷⁷⁶

Cette cybersécurité n'est pas à ranger sous l'étiquette de sécurité nationale mais plutôt du côté de la sécurité privée voire individuelle. Il faut attendre la parution du rapport parlementaire français rédigé par le député Pierre Lasbordes en 2006 cité au début de cette évocation des textes plus anciens pour se rapprocher un peu plus de la cybersécurité telle qu'elle est connue aujourd'hui⁷⁷⁷. Ainsi la sécurité de l'information en France de son émergence sous les traits de la sécurité informatique jusqu'à sa consécration par le livre blanc de 2008 a majoritairement opéré à travers les notions de cybercriminalité. Nous pourrons en tirer des conclusions concernant les différentes étapes de la transformation de l'information en enjeux

⁷⁷⁵ Extrait du compte rendu de la réunion de la commission des affaires étrangères, de la défense et des forces armées dans le cadre du projet de loi de finance 2008 du 7 novembre 2007.

⁷⁷⁶ Extrait de Déclaration de principes WSIS-03/GENEVA/DOC/4-F, *Construire la société de l'information : un défi mondial pour le nouveau millénaire*, sommet mondial sur la société de l'information, Genève, 12 mai 2004, article 35.

⁷⁷⁷ LASBORDES Pierre, 2006, op-cit.

de sécurité ce qui complète les développements menés jusqu'à présent. Il nous reste maintenant à voir le lien à la recherche afin de compléter la communauté épistémique.

D – La recherche en France face au tournant sécuritaire du cyberespace.

Cette sous-section est particulièrement importante car elle fait le lien avec le terrain de cette thèse : le monde académique français qui se consacre aux objets dérivés du cyberespace et plus largement à la sécurité de l'information. Les activités de recherche occupent une place importante dans la communauté « cyber »⁷⁷⁸, qu'il s'agisse de la recherche académique comme de recherche et développement.

Nous évoquerons donc principalement les fractures de la recherche labélisée « cyber » en France, la place centrale qu'y occupaient les chaires de recherche, le rôle social de la recherche avant d'en tirer les conclusions concernant notre définition de la communauté épistémique.

1 – Limites du terrain : fractures de la recherche « cyber » en France.

Il y a des fractures dans la recherche « cyber » en France. Ces fractures renvoient pour partie à des fractures ordinaires du milieu de la recherche et pour d'autres, elles sont la résultante de choix politiques. La première fracture est d'ordre disciplinaire. Il existe de la recherche en matière de « cybersécurité » dans les sciences et technologies et dans les sciences humaines et sociales. Toutefois ces ensembles se rencontrent assez peu sauf à la marge. Une pluridisciplinarité qui en viendrait à croiser et intégrer ces deux domaines et à avoir un apport significatif dans chacun des domaines est un projet qui se concrétise rarement.

La raison principale relève pour une part d'une absence de coopération antérieure et d'une économie de la recherche structurellement défavorable aux études disciplinaires croisées entre les domaines : la production de la recherche repose souvent sur l'emploi d'un doctorant et un doctorant fait le plus souvent sa thèse dans une seule discipline ou un seul domaine. L'autre part de cette division relève des objets scientifiques eux-mêmes. Si l'on devait

⁷⁷⁸ La recherche désigne ainsi l'ensemble des actions entreprises en vue d'améliorer et d'augmenter l'état des connaissances du phénomène « cyber ».

regrouper les objets scientifiques en grandes catégories : il y en aurait deux comme souvent. Il y aurait d'une part le travail scientifique sur l'impact de l'information dans sa dimension sécuritaire et un autre qui viserait à comprendre la « cybermenace » et éventuellement lutter contre elle. A priori la première thématique correspondrait aux sciences humaines, tandis que la seconde correspondrait aux sciences et technologies. Dans la réalité, chaque discipline académique travaille sur ses objets dans ces deux directions⁷⁷⁹. Cela produit de la concurrence y compris au sein des disciplines appartenant aux mêmes domaines.

Les trois raisons que l'on peut dégager du terrain pour adopter une perspective pluridisciplinaire et éventuellement « pluri-domaniale » sont le fait de bénéficier d'installations et/ou de plateformes expérimentales en commun, la complexité des objets étudiés ou encore le fait qu'un projet pluridisciplinaire soit utile pour récolter des fonds en vue de financer la recherche (soit à causes de critères publics ou internationaux, soit parce qu'elle est un argument intéressant pour solliciter des financements privés)⁷⁸⁰. La coopération scientifique est également facilitée par le réseau interpersonnel de chacun des chercheurs, et le critère de la proximité géographique. Cela est particulièrement vrai à l'échelle d'un territoire, mais peut s'avérer un déterminant essentiel au sein d'un établissement. Cette dernière assertion dépasse les frontières de la France. Si nous prenons l'exemple du programme en cybersécurité du King's College de Londres et de son *Cybersecurity Centre*. C'est un laboratoire qui les aspects sociotechniques de la cybersécurité autour de l'Intelligence Artificielle, de la cybersécurité formelle et stratégiques. Ce laboratoire se trouvent au croisement des départements d'informatique, des études de défense, des *War Studies*, des humanités numériques et du Policy Institute. La création de ce centre a été facilitée par la proximité des départements des *War Studies* et de l'informatique. En France, les projets pluridisciplinaires qui croisent les domaines croisant SHS et ST sont plutôt rares⁷⁸¹.

⁷⁷⁹ Informations tirées du recoupement de plusieurs entretiens avec des enseignants-chercheurs les 23 novembre 2012, 11 juillet 2014, 12 septembre 2014 (Cf. liste entretiens), ainsi des présentations de projets lors d'évènements scientifiques.

⁷⁸⁰ Même si des ponts existent entre les domaines. Il est par exemple possible aux Sciences et Technologies d'intervenir dans le domaine des Sciences Humaines et Sociales lorsqu'ils évoquent les enjeux éthiques ; de la même manière qu'il est possible d'intervenir dans le domaine des Sciences et Technologies avec l'étude des interactions entre l'humain et la machine.

⁷⁸¹ Il est possible par exemple de penser à la chaire Cyber Résilience Aérospatiale de l'armée de l'Air qui croise les thématiques des systèmes multi agents de cyber défense, autonomes & intelligents, de la cognition et de

Au-delà des enjeux disciplinaires, une autre fracture est due à la géographie. En étant caricatural, un panorama du terrain qui aurait presque pu être exhaustif de la recherche académique sur la cybersécurité en France peut s'obtenir en visitant trois villes et leurs alentours : Paris, Rennes et Lilles. Tous les acteurs de la recherche en cybersécurité montent à Paris pour de nombreux évènements quimporte la région d'où ils viennent. Ce qu'il n'y a pas à Paris, c'est le « pôle d'excellence cyber » situé en Bretagne et le forum international de la cybersécurité (le FIC, ex-forum international de la cybercriminalité) situé à Lille. C'est une structuration due à la création des premières chaires à Paris et en Bretagne dans les écoles militaires qui s'est accentué au moment du *Pacte Défense Cyber* en février 2014⁷⁸². Par rapport, à un tel dispositif, les autres régions de France interviennent sinon en seconde place en tout cas au second rang en termes de faculté d'accueil. Cette fracture pourrait se réduire dans le futur grâce au développement de « Laboratoire d'Excellence » (LabEx) spécifique ou de l'émergence du label de « Centre d'Excellence Défense et Stratégie » du ministère des Armées.

Une autre fracture qui n'est pas à négliger se situe dans la différence entre les recherches en milieu ouvert et en milieu clos. Ce milieu clos en matière de cybersécurité couvre une partie de la recherche et développement ainsi que de la recherche opérationnelle notamment dans des disciplines techniques ou opérant dans le cadre du secret industriel ou du secret de la Défense nationale⁷⁸³. Cette distinction emporte des conséquences sur l'insertion des chercheurs en question dans la communauté

Pour contrebalancer cette « fracture », la distinction entre « les chercheurs » et « les experts » ne s'est paradoxalement pas trop fait sentir au cours du terrain. Le milieu de la

l'ingénierie et management de la « supply chain cyber ». Ce qui en fait une chaire qui travaille à la fois dans le domaine des sciences économiques et de gestion, cognitives et informatiques. Si nous devions réfléchir à un objet commun inclusif capable de réunir l'ensemble des disciplines concernées, il faudrait sans doute travailler sur la normativité de l'information sous les angles socio-politique, juridique, organisationnel, technique et sociétal voire éthique. La norme représenterait un objet complexe intéressant capable de poser des questions épistémologiques et méthodologiques à la fois dans leur versant théorique mais aussi dans la mise en pratique.

⁷⁸² Dont l'axe 2 vise à préparer l'avenir en intensifiant l'effort de recherche tant technique et académique qu'opérationnel, tout en soutenant la base industrielle. Ce pacte prévoit notamment un pôle spécialisé chargé de répondre aux besoins du ministère et d'autres institutions en formation sera en développé en Bretagne, où se situent déjà le centre de la Direction générale de l'armement (DGA) Maîtrise de l'information, l'école des transmissions de Rennes, les Écoles de Saint-Cyr Coëtquidan, l'École navale de Brest et l'École nationale supérieure de techniques avancées-Bretagne. Cf. ministère de la Défense, *Pacte Défense Cyber*, 7 février 2014.

⁷⁸³ Pour rappel, dans le cadre de cette thèse, les informations sensibles qui ont pu être dégagées à l'occasion du terrain en sont considérées comme exclues d'office.

recherche en cybersécurité est particulièrement ouvert à la parole des experts que ce soit des experts « techniques » ou « stratégiques ».

Malgré les fractures disciplinaires, géographiques et celles résultants de l'ouverture de certains projets, peu de réelles difficultés se sont posées au moment d'étudier le terrain. Au début de la thèse et toute l'année 2013, la différence ne se faisait pas forcément trop sentir. Il y avait une petite dizaine de personnes concernées au plus haut sommet de l'État. Les événements militaires étaient ouverts au public et les groupes de travail des chaires de recherche étaient plutôt accueillant. Puis il y a eu une forme de replis durant l'année 2014 qui a été une grande période de transformation pour la recherche sur la cybersécurité en France.

Le milieu de la recherche s'est globalement refermé à ce moment-là dans l'ensemble de ses fractures (disciplinaire, géographique, ouverture). Les disciplines académiques ont commencé atteindre la masse critique pour se concentrer sur leurs cœurs de préoccupation plutôt que sur le caractère nouveau du phénomène. Les événements militaires ont cessé d'être ouverts à un public civil n'appartenant pas au ministère de la Défense. Les chercheurs des think tank n'ont plus été aussi présents dans les événements scientifiques qu'auparavant. Le *Pacte Défense Cyber* a opéré ensuite une forme de relative fermeture géographique dans la recherche académique sur le Nord/Nord-Ouest du territoire⁷⁸⁴.

Après cet exposé des quelques limites du terrain de recherche, il nous faut analyser le contenu de celui-ci.

2 – Les chaires de recherche « cyber » : « L'âge d'or », 2012 – 2017.

Trouver un angle d'attaque pour la recherche « cyber » en France n'est pas forcément aisés. Les fractures induisent en effet un paysage particulièrement morcelé. Il a donc fallu se pencher sur les motifs récurrents de celui-ci. L'un des motifs les plus caractéristiques de la recherche sur la cybersécurité que nous avons en France est la « chaire ». Dans le milieu universitaire chacun sait en quoi une chaire consiste. Il s'agit d'un poste permanent d'un professeur. Le sens du mot chaire quitte ici légèrement le sens universitaire classique. La chaire est un dispositif de financement et partenariat autour d'un projet de recherche. Bien que le

⁷⁸⁴ Fermeture d'autant mieux perçue en quittant la Bretagne pour les Bouches-du-Rhône en novembre 2014.

financement d'une chaire puisse être totalement public ou privé, le plus souvent, il s'agit ici d'un système de partenariat public-privé qui sera mis en place pour développer une recherche dite partenariale. Les bornes de cette partie de notre étude sont positionnées entre 2012 et 2017, période dans laquelle nous assistons à la structuration du champ autour de cette thématique.

N'ayant pu observer l'intégralité de ces dispositifs à l'échelle de la France toute entière, il y a surement quelques chaires qui ne font pas partie de cet échantillon soit par manque de temps, soit par manque de visibilité au sein de la communauté. A quelques exceptions près, la plupart de ces chaires sont prévues pour durer jusqu'aux environ de l'année 2020 pour le moment.

En dehors de ces dispositifs de recherche partenariale, la recherche académique en sciences humaines et sociales sur la question de la cybersécurité opère le plus souvent à l'échelle des individus. Il existe de nombreux autres réseaux et évènements en particulier le Forum international de la cybersécurité lancé en 2007. En 10 ans le forum est passé de 550 visiteurs lors de sa première édition de 2007 à environ 7000 lors de sa neuvième édition en 2017. Un autre évènement ponctuel intéressant est le Symposium sur la sécurité des technologies de l'information et des communications qui se déroule chaque année à Rennes.

Pour refaire l'historique, la naissance des chaires de recherche « cyber » en France est un processus assez récent qui remonte à l'année 2011 où la Fondation d'entreprise EADS et le Cercle des partenaires de l'Institut des Hautes Etudes de la Défense Nationale (IHEDN) lance la Chaire Castex de cyberstratégie⁷⁸⁵. Cette première chaire à une orientation géopolitique et portée par l'Université Paris 8 en particulier l'Institut français de Géopolitique (IFG). En juillet 2012, la Chaire de Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales est lancée avec un focus Science Politique élargi aux problématiques des études stratégiques ainsi qu'à la cybercriminalité⁷⁸⁶. Cette chaire est en particulier portée par le Centre de Recherche des écoles de Saint-Cyr Coëtquidan (CREC). L'année 2014 voit la création de chaires plus généralistes qui interviendront également dans la recherche sur la cybersécurité. Ainsi, la chaire Economie

⁷⁸⁵ La chaire est alors confiée à François Géré. La chaire change de titulaire début 2013 au profit de Frédéric Douzet. La chaire durera jusqu'à début 2018.

⁷⁸⁶ La chaire est confiée à Daniel Ventre jusqu'en 2017. Jean-Paul Laborde est désigné nouveau titulaire. Cette chaire est membre du pôle d'excellence cyber.

de défense organise sa leçon inaugurale en janvier 2014⁷⁸⁷. Parmi les chaires plus généralistes, en septembre 2014, l’IEP de Bordeaux et l’Université de Bordeaux se sont associés avec Dassault Aviation, Safran et Thales pour créer une chaire Défense & Aérospatial⁷⁸⁸. En octobre 2014, L’École navale, Naval Group, Thalès et Télécom Bretagne (IMT Atlantique) ont lancé la chaire de cyberdéfense des systèmes navals. Cette chaire se concentre en particulier sur les aspects techniques de la cybersécurité⁷⁸⁹. En janvier 2016, c’est la Chaire Cyber CNI de l’Institut Mines-Télécom qui est créée dédiée au domaine de la cybersécurité des infrastructures critiques⁷⁹⁰. Cette chaire est pluridisciplinaire. En juin 2017, l’Armée de l’air, Dassault Aviation et Thalès lancent la chaire de cyber-résilience aérospatiale⁷⁹¹. Cette chaire pluridisciplinaire est basée à l’Ecole de l’air dans les locaux du Centre de recherche de l’armée de l’air.

Les conditions de financements dépendent à chaque fois de contextes historiques et structurels locaux qui relèvent des établissements d’accueil des dispositifs. Néanmoins cette tendance au partenariat public-privé s’inscrit dans la tendance européenne sur toute cette période⁷⁹². Sauf exception de la chaire de cyber-résilience aérospatiale, il est possible de voir une tendance à la multiplication des mécènes sur chacun des projets de chaires au fur et à mesure de l’avancement du temps et de la progression de la thématique. Il est également possible de constater que certains groupes d’entreprise comme Thalès sont très présents dans ce type de projets quel que soit le type de discipline de la chaire. Par ailleurs, les trois grandes écoles d’officiers ont chacune leur chaire dédiée avec trois portages disciplinaires différents.

Il y a trois grandes tendances qui se dégagent de l’activité des chaires : d’une part, la valorisation de la recherche (aux travaux d’événements et de publications) ; d’autre part, l’encadrement des jeunes chercheurs (soit avec des réseaux de jeunes chercheurs soit en encadrant directement des thèses) ; et enfin, le pilotage ou l’association dans le développement

⁷⁸⁷ Le titulaire est Jean Belin. Le titulaire adjoint est Julien Malizard.

⁷⁸⁸ Les sociétés Ariane Group et CEA/DAM ont rejoint la chaire en 2017. Le responsable exécutif de la chaire est Jean-Marc Laurent.

⁷⁸⁹ Le titulaire de la chaire est Patrick Hébrard. Cette chaire est membre du pôle d’excellence cyber.

⁷⁹⁰ Le porteur de projet est Frédéric Cuppens. Cette chaire est membre du pôle d’excellence cyber.

⁷⁹¹ La chaire est confiée à Pierre Barbaroux et à Paul Théron.

⁷⁹² DUBO Orlane, *Analyse comparée de la recherche en matière de cyberdéfense militaire*, Rapport du Centre de recherche de l’armée de l’air, 2015, 51 p.

d'offres de formation. En plus de son positionnement disciplinaire, chaque chaire a un portage particulier sur ce domaine-là aussi.

Au niveau de la production scientifique, malgré une forte capacité à valoriser des travaux de recherche et une grande visibilité de ces dispositifs, la production de connaissance n'est pas majoritairement le fruit de ceux-ci. En effet, l'encadrement de la plupart doctorants se fait principalement dans les établissements d'enseignements supérieurs hors des dispositifs spécifiques (notamment en sciences et technologie, mais également en sciences humaines et sociales). Il y a plusieurs raisons à cela. Toutes les chaires « de recherche » ne choisissent pas d'encadrer des doctorants. Toutes les chaires qui choisissent d'avoir des doctorants ne sont pas forcément hébergées dans un établissement disposant d'une école doctorale ou affiliée à l'une d'elles (c'est notamment le cas de certaines écoles militaires). Par ailleurs, la position scientifique disciplinaire ou spécialisée de certains dispositifs réduit l'assiette du potentiel d'accueil. Du point de vue des chercheurs confirmés, les structurent en chaire fonctionne le principe d'un ou deux titulaires, voir éventuellement un ou deux employés. Les autres chercheurs confirmés sont « associés à la chaire », mais n'en font pas partie directement et ne consacre qu'une partie de leur temps à ce partenariat. Celui-ci n'étant pas déterminant de leur emploi. Dès lors, un chercheur confirmé peut intervenir comme co-encadrant ou co-directeur de thèse, conférencier ou coauteur sur un livrable scientifique, mais il n'a pas d'intérêt particulier à inscrire l'ensemble de sa production dans une chaire⁷⁹³. Enfin, la démarche de production d'une chaire partenariale est tournée vers la valorisation. Dès lors, une chaire de recherche partenariale dispose d'un éventail d'actions beaucoup plus large. Ici les dispositifs spécifiquement dédiés à la cybersécurité apparaissent majoritairement comme une interface permettant de créer des lieux de convergence et de visibilité pour les travaux des experts, plutôt que comme des lieux de production des travaux des experts.

3 – Les aspects sociaux des évènements scientifiques, source d'influence communautaire.

Mise à part les activités de production de connaissance et de formation, l'ensemble de ces dispositifs s'est particulièrement distingué dans la valorisation des connaissances et tout

⁷⁹³ Cette inscription peut même réduire l'étendue du public touché par la publication si la chaire est spécialisée (le label déterminant une partie de la réception du travail indépendamment de ses qualités intrinsèques).

particulièrement par l'organisation d'évènements à caractères scientifiques qui ont réussi à former une communauté intéressante à analyser, notamment du point de vue du discours. C'est sur cette dimension que portera le présent propos.

En effet, au-delà des chercheurs internationaux et nationaux qui assistent à ces conférences, le public de celles-ci est particulièrement riche de profils divers et variés. C'est tout particulièrement le cas à Paris. Il est ainsi possible d'y rencontrer des chercheurs, mais aussi des cadres issus de l'industrie de l'armement, des télécommunications ou de l'informatique. Il est aussi possible d'y rencontrer des cadres issus de l'administration (Armées, Police, Diplomatie). Il y a également des avocats, des banquiers. Parfois, il est possible d'y trouver des hackers, des militants, voire des personnes faisant carrière dans la politique.

Dans cet environnement complexe, l'évènement scientifique revêt un caractère particulier car il peut plus difficilement devenir une conférence de « spécialistes » sans perdre la grande majorité de son public. Le rôle du langage est ici de fédérer le public de l'évènement en question. En tant que tel, le langage « cyber » et son impossible définition sont ici un excellent moyen d'entretenir une zone d'échange autour des intérêts de chacun des membres du public. Il permet également de mettre les gens en contact.

C'est ainsi que la conférence scientifique devient un lieu de sociabilisation ou de médiation pour tous les cadres des services qui vont être amenés à coopérer ensemble sur l'enjeu en question. Pour un fonctionnaire affecté en poste dans une administration, il peut par le truchement de la conférence rencontrer un homologue d'une autre administration qui travaille sur le domaine en question. Il en va de même pour les entreprises.

Dans un autre registre, elle permet au chercheur de faire venir le terrain à lui et par là même de diminuer le coût d'ouverture de celui-ci pour mener des enquêtes ou proposer son expertise. D'un outil de simple valorisation, elle peut devenir un outil favorable à la production de connaissance. Cela est d'autant plus utile lorsque l'objet d'étude est un objet relatif à la sécurité et « nouveau ». Le niveau de qualité scientifique de la conférence et des intervenants est un élément de légitimation supplémentaire qui facilite les rencontres. Le sujet de la conférence en lui-même, le lieu, le fait que la conférence soit organisée par une personne ou

collectif identifiable sont autant d'indicateurs favorables au développement de cette communauté d'intérêts.

Cet aspect social de la recherche apparaît comme l'un des premiers vecteurs de la communauté épistémique de la sécurité de l'information qui se crée dans les publics de ces conférences. A l'échelle du discours, principal médiateur d'une idée évoluant dans son propre espace sémantique cela fait autant d'experts à convaincre de la définition des termes d'un problème avec un haut degré de visibilité avec un haut degré d'incertitude de l'enjeu⁷⁹⁴. La recherche semble avoir ici pour fonction d'organiser le discours de manière à favoriser son caractère audible par le plus grand nombre. Par analogie, sans aller jusqu'à une comparaison avec les salons, cette sociabilité pourrait en partager certains traits : l'aspect codifié de l'évènement à caractère scientifique, la récurrence des rencontres tout au long de l'année, l'hospitalité matérialisée ici pour le public dans l'éventuel buffet, voir dans l'hospitalité de la prise en charges des frais de transport et logement du conférencier.

Conclusions de chapitre.

Être un membre de la communauté épistémique de la sécurité de l'information, c'est être quelqu'un avec qui il est possible d'en parler. Cette aptitude à la controverse repose sur la maîtrise du discours. La sélection des membres de la communauté épistémique ne passe pas tant par une sélection active et un processus de formation que par des logiques de reconnaissance et d'exclusion médiatisées par le langage. La définition de la perception d'un problème et la controverse qu'elle implique forment les limites de l'espace sémantique où la communauté peut hiérarchiser ses membres. Cette hiérarchie communautaire existe en complément de la hiérarchie propre de chacun des acteurs. Dans un contexte où il est impossible pour un individu d'apprécier les qualités de la production de connaissance dans une discipline académique ou technique où il n'est pas formé, cette reconnaissance opère moins du fait de la qualité des connaissances produites que de la capacité à les valoriser au travers d'un réseau grâce à son activité.

En utilisant le concept de communauté épistémique centré sur le discours, le chapitre a mis en lumière des phénomènes d'influences qui pouvaient exister dans celui-ci. En effet, cette

⁷⁹⁴ ZITO Anthony R, 2001, op-cit. ; RADAELLI Claudio M., (1998), 2017, op-cit.

étude nous a permis de poser les jalons d'un processus de transformation en enjeu de sécurité à l'échelle d'un état et de mettre en avant différents acteurs qui pouvaient y contribuer soit en formulant des concepts (Le cas de la RAND Corporation), soit en médiatisant l'enjeu concerné (le rôle des structures de recherches partenariales), soit en fournissant directement une prestation technique associée à l'enjeu (Le cas des CERT ou CSIRT). Chacun de ces acteurs possède sa propre forme de légitimité. Ces acteurs viennent s'inscrire dans les limites du discours afin de former une communauté épistémique centrée sur l'enjeu dont il est possible de situer un ancrage dans l'acteur régional de référence. La communauté désigne ainsi l'ensemble des locuteurs du discours savant. Elle ne se limite pas à une seule organisation mais existe en tant que communauté qui existe malgré les liens bureaucratiques de chacun des acteurs de celle-ci. Par son ouverture et ses différents niveaux de liens avec les experts nationaux et internationaux de tout domaine, cette communauté épistémique de la sécurité de l'information cristallise une partie des canaux d'influence. Lesquels peuvent modifier la perception politique d'un problème.

Cette communauté particulière de la sécurité de l'information en France se développe autour des discours et notamment le discours qui allie la sécurité de l'information au langage « cyber » comme un intérêt de l'État. Ce discours se développe à l'étranger notamment aux États-Unis dans les années 90, et commence à émerger durant la même période en France à quelques années de différence. Même si la consécration de ce discours s'opère en 2008. Les premières occurrences sont plus anciennes et montrent une circulation de l'idée entre plusieurs champs. La transformation de sens du cyberspace vis-à-vis d'un intérêt régional peut être datée à la parution d'une étude de la RAND en 1993. Sa montée en puissance pour devenir l'un des paradigmes dominants pour penser les enjeux de la sécurité de l'information se déroulerait entre cette période et l'année 2007. Sa consécration est effective en France en 2008 et c'est seulement alors que la communauté épistémique peut se développer. Il est en effet important de souligner que c'est bien une impulsion de l'acteur régional qui décide de consacrer cet enjeu par ce langage particulier qui entame le développement de l'intérêt des autres acteurs utilisant le même langage. La communauté désigne le phénomène dynamique de redistribution des rapports de force dans l'espace sémantique relatif à un enjeu de la sécurité de l'information.

L'impossible définition technique du cyberspace, son pouvoir évocateur et sa faculté à être réduite à un seul préfixe susceptible d'être adossé à n'importe quel terme semble renforcer

la capacité de la communauté à fédérer l'expertise provenant de divers milieux autour de lieu de rendez-vous que fournissent les instruments spécifiquement dédiés des champs concernés qu'il s'agisse de recherche scientifique ou d'une autre forme d'expertise. Il n'en sera pas moins de variable permettant de hiérarchiser la communauté. La communauté épistémique ne distribue pas la force en fonction l'excellence ou de la pertinence des approches expertes mobilisées, mais au contraire. La personne qui domine la concurrence discursive au sein de la communauté sera celle qui parvient le mieux à traduire ses conclusions logiques « expertes » dans le langage naturel sans pour autant renier. Autrement dit, la communauté épistémique et son influence ne dépendent pas tant de leur production de connaissance que de leur capacité à vulgariser cette dernière. Et, il n'y a pas de meilleur outil qu'un concept polymorphe et sténographique pour disposer d'une influence maximale.

Conclusions partielles.

Cette première partie du manuscrit avait pour objet de comprendre le phénomène linguistique que constitue le cyberespace et ses termes dérivés. Il a en a abordé le contenu et la diffusion en analysant la notion de cyberespace, l'impact normatif de ses mutations et une partie de son utilisation parmi les experts en France. Le phénomène linguistique analysé consiste en l'emploi de mot nouveaux formés à partir d'un préfixe commun (« cyber- ») pour traduire une idée selon laquelle l'information est un objet de sécurité.

Dans le premier chapitre, un lien a été établi entre ce phénomène et le mot cyberespace comme étant l'origine du préfixe précité. Une étude de cette notion de cyberespace a été menée en travaillant sur les origines du terme et les héritages dont il a pu bénéficier dans sa création entre 1982 et 1984, ainsi que son rapport à la technique. Les principales conclusions de ce chapitre décrivent que le cyberespace est une notion littéraire aux frontières peu définies et capable d'englober nombre de thématiques. En l'ayant créé comme un théâtre pour ses histoires, l'auteur William Gibson a forgé un mot nouveau doté d'un pouvoir évocateur puissant mais sans définition technique claire. Ce terme peut être source de confusion entre différents objets techniques d'une réalité complexe. La diffusion de l'emploi du mot au-delà de l'œuvre de fiction a renforcé ce phénomène. Le cyberespace d'aujourd'hui a perdu son sens littéraire pour devenir une métaphore dont le sens résulte d'une sorte de mélange entre l'information, Internet et le World Wide Web. Cela rend toutes les tentatives de définitions très difficiles. Une

telle définition semble impossible, nous ajoutons même qu'elle ne pourrait se faire qu'au détriment du pouvoir évocateur de la notion. La recherche d'une définition au sens technique n'est pas souhaitable. Et les tentatives de définitions auxquelles conduisent logiquement les travaux descriptifs doivent être considérées de façon particulièrement critique, voire avec méfiance. En explorant les origines matérialistes de la technique et de l'information, ce chapitre est parvenu à la conclusion que le sens du cyberespace n'avait rien de technique, mais qu'il devait se comprendre comme une forme de pensée technique ou de technicisme. En tant que fiction techno-politique, le cyberespace traduit une forme de perception impossible des phénomène techniques de l'information grâce à une spatialisation simplifiée et totale de l'idée d'information. Dans cet espace, la sécurité apparaît comme une réponse logique à une absence de maîtrise de l'information. En tant que métaphore, le cyberespace vient mobiliser des figures discursives récurrentes et notamment personnages conceptuels et des artefacts techniques pour alimenter sa démonstration. Toutefois, l'analyse du phénomène ne serait pas complète sans une analyse des termes créé à partir du cyberespace (ou cybtermots). Le chapitre 2 propose une mesure de la diffusion des termes dérivés du cyberespace au travers de l'analyse logométrique de leurs impacts normatifs dans les publications officielles en français entre 2001 et 2016 portant sur les journaux officiels de la République française, de l'Union européenne et du système de documentation de l'Organisation des Nations Unies. Cette première analyse a suivi d'une étude de même nature et même période sur deux corpus de la presse en langue française disponibles sur les plateformes Factiva et Google. Ces études ont permis de démontrer que sur la période considérée les mutations des cybtermots et de leurs contextes d'emploi étaient caractérisées de manière très nette par l'idée de sécurité. Lorsqu'un terme avec le préfixe « cyber » est utilisé, c'est la plupart du temps pour décrire un enjeu de sécurité spécifique autour de l'information. Par ailleurs, ce phénomène croît globalement dans le temps, mais sa composition évolue. Ces contextes d'emploi mettent en avant l'acteur régional au détriment de la vie internationale. L'individu ne transparaît qu'au niveau de la presse et de l'ONU. Parmi les enjeux principaux dégagés par l'étude des textes, ont été retenus la menace, la protection, la sécurité, la criminalité et la défense. Ce sont les enjeux principaux du discours, suivis par une série d'enjeux périphérique que sont la gouvernance, la gestion des flux de données (et l'accès) ainsi que la résilience. L'ensemble de ces variations s'inscrivent dans le cadre d'un discours qui allie la sécurité de l'information au langage « cyber » comme un intérêt de l'État. Grâce à une relecture de la communauté épistémique comme communauté discursive, la communauté qui porte et se coconstruit avec ce discours peut être regardée comme la communauté

épistémique de l'information. Sans revenir, sur l'analyse développée dans le chapitre 3, cette approche du discours permet ainsi de classer et hiérarchiser les différents membres de la communauté. Plusieurs exemples d'acteurs de la communauté épistémique travaillant sur l'enjeu de la sécurité de l'information en qualité d'experts ont pu être identifiés. Ce discours se développe à l'étranger notamment aux États-Unis dans les années 90, et commence à émerger durant la même période en France à quelques années de différence. Prenant petit à petit de l'importance dans divers cercles de l'État, il sera consacré par le livre blanc sur la défense et la sécurité nationale de 2008. Toutefois cette consécration opère une greffe du langage sur des phénomènes relativement anciens qui sont concomitant à l'introduction de l'outil informatique dans l'administration et dont les racines remontent plus loin encore. Il ne peut pas être considéré comme spécifique à la France dans la mesure où l'enjeu est répandu dans la plupart des États. La France sert ici d'ancrage afin de montrer comment les influences techniques et scientifiques circulent d'un État à un autre et peuvent être l'objet de phénomène d'influence. Dans ce domaine, comme de nombreux États du monde, la France fait l'objet d'une influence américaine sur les plans politiques, techniques, scientifiques et culturels qui détermine une partie de la structuration de la communauté épistémique.

Ces trois chapitres nous permettent de mobiliser l'ensemble de notre approche discursive visant à circonscrire les grandes lignes de l'espace sémantique du cyberespace. Le postulat de départ qui voulait que le cyberespace et ses termes dérivés participent d'un même phénomène discursif n'a pas été remis en cause par les résultats obtenus. Cette première partie de nos développements a expliqué ce qu'était le cyberespace et la prolifération de formes et de sens dont il fait l'objet. Elle a également permis de découvrir quelles représentations étaient principalement véhiculées par les usages de ce langage. Toutefois, ces réponses ne sont que la première étape pour comprendre le cyberespace sous l'angle des Relations Internationales et déterminer ce qu'il peut apporter à la compréhension de celles-ci. Laquelle passera immanquablement par une sortie du discours « cyber » pour se focaliser sur la sécurité de l'information.

Cette réponse à la problématique par le passage du « discours » (« cyber ») à son « objet » (la sécurité de l'information) est le rôle de la seconde partie de ce manuscrit.

Titre : Relations Internationales et cyberespace, théories et acteurs asymétriques

Mots clés : *Science politique, Relations Internationales, Etudes critiques de sécurité, analyse de discours.*

Résumé : Partant du phénomène de la prolifération du « cyberespace » et de l'ensemble des termes qui en sont dérivés, cette thèse interroge la prise en considération de la sécurité de l'information et de son influence sur les Relations Internationales.

Afin de répondre à cette question, cette recherche croise la combinaison pragmatique conduite par les problèmes avec une analyse de discours mobilisant plusieurs approches méthodologiques, notamment la logométrie et les communautés épistémiques.

Parmi ses principaux résultats, cette thèse déconstruit les récits qui entourent le cyberespace de ses origines littéraires à son réemploi dans l'administration. Elle quantifie un accroissement de sa diffusion pour définir un ensemble de préoccupations liées à la sécurité de l'information. Après l'analyse de discours sous l'angle des études critiques de sécurité combinée à l'étude de ses réceptions dans les Théories des Relations Internationales, la thèse propose de comprendre la sécurité de l'information notamment sous l'angle des théories cyberpolitiques de Nazli Choucri et de la théorie de l'acteur-réseau.

Title : International Relations and cyberspace, theories and asymmetric actors

Keywords : *Political Science, International Relations, Critical Security Studies, Discourse Analysis.*

Abstract : Based on the phenomenon of the proliferation of "cyberspace" and all the terms derived from it, this thesis questions the consideration of the security of information and its influence on International Relations

To answer this question, this research combines problem-driven pragmatism with a discourse analysis involving several methodological approaches, including logometry and epistemic communities.

Among its main results, this thesis deconstructs the narratives that surround cyberspace from its literary origins to its re-employment in administration. It quantifies an increase in its dissemination to define a set of information security concerns. After the analysis of discourse from the angle of Critical Securities Studies combined with the study of its receptions in the Theories of International Relations, the thesis proposes to understand the security of information especially from the angle of the Nazli Choucri's cyberpolitics theories and the actor-network theory.

THESE DE DOCTORAT DE

L'UNIVERSITE DE RENNES 1
COMUE UNIVERSITE BRETAGNE LOIRE

ECOLE DOCTORALE N° 599
Droit et Science politique
Spécialité : *Science politique*

Par

Yves Auffret

Relations Internationales et cyberespace, théories et acteurs asymétriques
Etude pragmatique de la sécurité de l'information par l'analyse de discours

TOME 2 – Seconde partie, conclusions, annexes

Thèse présentée et soutenue à Rennes, le 6 novembre 2019
Unité de recherche : Institut du Droit Public et de la Science Politique, UR1_RS438

Rapporteurs avant soutenance :

THIERRY BALZACQ
Professeur à l'Institut d'Etudes Politiques de Paris

JEAN-VINCENT HOLEINDRE
Professeur à l'Université Paris II, Panthéon-Assas

Composition du Jury :

THIERRY BALZACQ
Professeur à l'Institut d'Etudes Politiques de Paris

JEAN-VINCENT HOLEINDRE
Professeur à l'université Paris II, Panthéon-Assas

FREDERIC LAMBERT
Professeur à l'université de Rennes 1

JENNY RAFLIK-GRENOUILLEAU
Professeure à l'Université de Nantes

Directeur de thèse
BERNARD BRUNETEAU
Professeur à l'université de Rennes 1

Université de Rennes 1
ECOLE DOCTORALE N° 599 - Droit et Science politique

RELATIONS INTERNATIONALES ET CYBERESPACE THEORIES ET ACTEURS ASYMETRIQUES

Etude pragmatique de la sécurité de l'information par l'analyse de discours

TOME 2 – SECONDE PARTIE, CONCLUSIONS, ANNEXES

Par Yves Auffret

Thèse présentée en vue de l'obtention du doctorat en Science Politique

Sous la direction du Professeur Bernard Bruneteau

Membres du jury :

M. Thierry Balzacq, Professeur à l'Institut d'Etudes Politiques de Paris (rapporteur)

M. Jean-Vincent Holeindre, Professeur à l'université Paris II, Panthéon-Assas (rapporteur)

M. Frédéric Lambert, Professeur à l'université de Rennes 1

Mme Jenny Raflik-Grenouilleau, Professeure à l'université de Nantes

M. Bernard Bruneteau, Professeur à l'université de Rennes 1 (directeur)

6 novembre 2019

Partie II – Sécurité de l’information dans les Relations Internationales : De l’enjeu de sécurité à un acteur en réseau.

« Si nous acceptons l’idée qu’un processus de mondialisation est en train de se produire alors nous n’avons plus besoin de théorie des relations internationales. [...] A l’inverse, dire que le noyau dur de l’entreprise consiste à théoriser les relations internationales revient à sérieusement mettre en doute l’idée même qu’il puisse y avoir quelque chose comme un processus de mondialisation. »

Ian CLARK⁷⁹⁵

⁷⁹⁵ CLARK Ian, *Globalization and International Relations Theory*. Oxford University Press, 1999, p. 1.

Ce dilemme de Clark à propos de la mondialisation résume assez bien la position difficile du chercheur qui fait face à un phénomène de cyberespace tel que décrit dans la première partie de ce manuscrit. En tant que phénomène global, sans être aussi général que le concept de mondialisation, le phénomène du cyberespace renvoie à l'étude d'un certain nombre de faits et de concepts qui amènent à sortir d'une vision institutionnelle de l'acteur régional.

C'est toute la question de cette seconde partie. Pour comprendre le cyberespace sous l'angle des Relations Internationales et déterminer ce qu'il peut apporter à la compréhension de celles-ci, encore faut-il que les Théories des Relations Internationales puissent se saisir d'un tel objet et que ce dernier n'aile pas à l'encontre de celles-ci. A la lumière des développements de la première partie, il serait possible de douter des capacités des Relations Internationales à prendre en compte le cyberespace, tant ce discours amène une forme de remise en question de l'ensemble des éléments constitutifs de l'État. L'idée défendue dans cette partie est qu'une telle appréhension est possible à condition d'adopter la bonne combinaison de théories

Dans un premier temps (**Chapitre 4**), le phénomène du langage « cyber » sera étudié comme un discours de sécurité à travers la caractérisation de ses principes de fonctionnement. Cette caractérisation supposera de faire le lien entre les théories et l'objet de référence, ainsi qu'entre l'emploi d'un langage et l'objet de référence. C'est la raison pour laquelle ce chapitre évoquera tout d'abord quelques éléments du discours qui serviront à construire une approche discursive de la sécurité de l'information. Cette grille d'analyse reposera essentiellement sur la sécurisation sous l'angle de l'Ecole de Copenhague. Après une critique de cette grille, le propos se centrera sur la réception de la sécurité de l'information dans les Relations Internationales.

Dans un second temps (**Chapitre 5**), cette partie abordera les questions qui émergent de des recherches précédentes tout en faisant le lien avec la première partie des développements. Il y aura principalement quatre questions qui intéresseront l'étude des Relations Internationales : celle du langage « cyber », celle de la technologie et de l'information comme objet d'étude, et celle de l'agentivité. Après quoi, de façon à répondre à la problématique, le chapitre 5 proposera une combinaison de théories destinées à comprendre la sécurité comme enjeu de l'information dans les Relations Internationales.

Chapitre 4 – Le cyberespace, un discours de sécurité consacré à l’information parmi d’autres.

« La force est le produit de la nécessité : la sécurité entretient et encourage la faiblesse. »

H. G. WELLS⁷⁹⁶

Le présent chapitre a pour but de faire le lien entre le phénomène du langage analysé (les mots en « cyber-»), l’objet qu’il sécurise (l’information) et les différentes théories pouvant être utilisées comme explications de ce phénomène. Lesquelles représentent le moyen que nous avons sélectionné pour répondre à notre question de recherche. Seulement, dans le champ sémantique, le lien entre ces trois éléments n’est pas immédiat car il opère à la rencontre d’une multitude de phénomènes dans plusieurs contextes nationaux différents. Il n’existe pas de traduction de l’empirie dans une seule théorie. Au contraire, le phénomène analysé peut utilement trouver son explication dans plusieurs théories.

Ce pluralisme existe déjà par le langage. Par exemple, la cybersécurité est un terme large. En général, il fait référence à l’intégrité des réseaux électroniques, à leur utilisation prévue et à toutes les données et systèmes associés. Cela pourrait inclure n’importe quoi, de l’hygiène ordinaire des systèmes personnels à la défense des réseaux militaires de la guerre électronique. Il peut également faire référence à la fois à la défense de ses propres réseaux ou le développement ou l’utilisation de capacités offensives contre un adversaire. Dès lors, l’ensemble théorique mobilisé doit être en mesure de percevoir le sens d’une telle notion. Et il en va de même pour l’ensemble des autres termes qui constituent le phénomène du langage « cyber »

Au cours de cette recherche, ont déjà été évoqués les concepts sténographiques et polymorphe de Jean-Claude Passeron, toutefois ces définitions n’opèrent que pour la partie du phénomène qui se situe dans le champ sémantique au niveau des artefacts linguistiques. Si nous pouvons mobiliser ces éléments théoriques pour éclairer la pluralité de sens du phénomène au niveau politique. Nous ne pouvons pas pour autant en faire un phénomène de Relations

⁷⁹⁶ WELLS Herbert George (1895), *La Machine à explorer le temps*, Chapitre VI, Le Crépuscule de l’humanité, Paris, Larousse, 2017, p. 47.

Internationales sans avoir recours à une théorie qui permette de traduire ce pluralisme de l’empirie en phénomène observable. Afin de parvenir à une explication de l’ensemble du phénomène, le pluralisme suppose d’avoir recours à une approche combinatoire que nous avons identifiée lors de nos propos liminaires. Toutefois, pour en arriver à ce stade de la réflexion, il faut parvenir à appliquer une théorie qui permette de passer de l’ensemble de discours analysé à un phénomène politique.

Autrement dit, sorti du discours, qu’est-il possible de déduire et de construire avec le cyberespace ? Cette question sera l’un des fils directeurs de toute la seconde partie de ce manuscrit. Un tel questionnement suppose que l’on puisse faire le lien entre les théories et l’objet de référence, mais il suppose également que l’on puisse faire le lien entre l’emploi d’un langage et l’objet de référence.

Ce chapitre a pour but d’établir ce lien en analysant le cyberespace comme un discours de sécurité. La première section a pour but d’approfondir les éléments relatifs au contenu du discours. La deuxième section vise à construire une approche discursive du cyberespace puis d’élargir cette approche à l’ensemble des discours concernant la sécurité de l’information. Enfin la troisième section donnera lieu à une analyse de l’influence de la thématique de la sécurité de l’information sur les objets des Théories des Relations Internationales.

Section 1 – Des éléments du discours : menace, dépendance, valorisation de l’information.

Si on regarde le discours, la cybermenace peut être décrite comme tout ce qui peut arriver de mauvais par le biais de l’information numérisée. C’est la dimension la plus visible. La dimension « cyber » de la menace est comprise comme un moyen. Pourquoi « information numérisée » plutôt qu’ « informatique » ? Car la menace n’est pas la machine elle-même mais découle nécessairement d’une utilisation particulière, la menace est informationnelle.

D’un point de vue très caricatural, le fait de subir une agression commise à l’aide d’un écran d’ordinateur employé comme une arme contendante improvisée n’entre pas dans le spectre de la cybermenace. Ou encore, le fait d’attaquer avec une bombe les câbles sous-marins et causer une faille dans le réseau d’un autre État pourrait être considéré comme une attaque

classique ou éventuellement comme un acte préparatoire à une cyberattaque, mais ne pourrait constituer la cyberattaque elle-même. A l'inverse utiliser une attaque visant à neutraliser un système informatique pour entraîner des dommages sera considéré comme une cyberattaque.

La présente section abordera dans un premier temps le caractère subjectif de la menace par le biais de sa définition discursive, avant d'un élément objectif de celle-ci : l'information. Laquelle sera comprise sous l'angle de la dépendance, puis de sa valorisation.

A – Définition discursive de la menace et désignation de l'adversaire : une synthèse globale de nombreux enjeux de sécurité.

La menace n'est pas strictement définie par un objectif (comme la notion de terrorisme), par un outil ou l'arme (comme par exemple les menaces nucléaire, radiologique, biologique et chimique), par un acteur ou par un type d'atteinte et de dommages. Il lui manque quelque chose. L'agression doit venir de l'information numérisée : elle est principalement définie par le vecteur employé. A partir du moment, où l'attaque ou la menace « provient » du réseau, elle peut être qualifiée de « cyber ».

Cette spécificité du langage est une composante de la spatialisation de l'information. Le langage participe de la « naturalisation » de la menace dans la construction d'une représentation du cyberspace comme espace naturellement dangereux. L'analyse du discours nous apprend que la menace est un élément naturel de l'information. Cela en fait une préoccupation perçue comme naturelle pour les acteurs. Définir la menace est ainsi une question complexe qui illustre bien toute la transversalité de la représentation. Deux types de question structurent la définition de la menace : d'une part, la nature de la menace et d'autre part, l'acteur menaçant. Dans un contexte où tout le monde peut être une victime d'un mauvais usage de l'information, la question de la nature de la menace joue un rôle important dans la délimitation des moyens destinés à y répondre.

1 – Des caractéristiques de la menace, entre importance et incertitude.

Le premier caractère, voire parfois le seul dont il est fait explicitement mention dans le texte, est que la menace constitue un « enjeu important ». Dans les discours institutionnels cette importance est variable, il est toutefois possible d'affirmer que l'idée de cybermenace et plus généralement la cybersécurité connaissent aujourd'hui un statut comparable au terrorisme dans

les préoccupations des différents acteurs (même si de nombreux points de convergence existent entre les deux thématiques). En tant qu'enjeu important, la cybermaneace constitue principalement une crainte environnementale qui n'emporte pas nécessairement à première vue de désignation d'un ennemi spécifique.

L'analyse de discours tendrait à figurer une menace à caractère total capable d'affecter tous les aspects de l'information ou dépendants de l'information. A l'image de l'espace dans lequel elle évolue, la cybermaneace est dynamique. Elle évolue vers de nouvelles formes et elle est présentée en prolifération. Le niveau technique de la cybermaneace est réputé croître. Tandis qu'à l'inverse, leur compréhension est présentée comme en diminution. La menace est présentée comme globalement sous-estimée (bien que l'enjeu de la menace constitue sans doute le thème majeur du discours, ainsi que son principal objet de travail et d'observation, jusqu'à faciliter le développement du secteur économique de la sécurité de l'information).

Sur le plan technique, la cybermaneace consacre un principe général d'incertitude. Tout équipement qui a été, est, sera ou pourra être « connecté » est ou sera susceptible d'être un vecteur de menace. Tout système peut être piraté. Tout code est susceptible de corruption. Toute chiffrement peut être potentiellement cassée. Toute donnée peut être copiée, dérobée ou utilisée. Le principe est celui du continuum entre victime et menace au plan de la technique, si tout système, code, chiffrement, donnée peut-être victime d'une cybermaneace, il devient lui-même cybermaneacant. La cybermaneace repose sur une logique symbolique d'infection et de contamination. Il est donc plus raisonnable en l'absence d'informations fiables de considérer tout élément technique comme potentiellement menaçant.

La principale stratégie de définition repose sur un découpage de cette menace de l'information en différentes menaces plus précises. De nombreuses typologies sont ainsi construites afin de présenter ce que l'on suppose être les différentes variations de la menace. Le critère de détermination le plus souvent utilisé semble ici la malveillance réputée du comportement en question. Toutefois, il existe d'autres variantes qui ne cherchent pas tant à appréhender la menace par le biais des comportements menaçants que par les acteurs (agresseurs, cibles) ou par la technique (virus, logiciels malveillants). Toutefois, en l'absence de listes exhaustives d'acteurs, la description des menaces relève le plus d'une typologie non-exclusive des emplois. Ces typologies peuvent dépendre des différents secteurs et cibles que l'émetteur de la typologie considère comme importants. Ils peuvent également être un

inventaire des dispositifs techniques. La cyberattaque⁷⁹⁷ fait partie des plus grandes préoccupations. Nous retiendrons une définition générique de l'attaque comme une action malveillante contre un dispositif informatique par le biais des réseaux. Ces attaques sont caractérisées par la mise en œuvre de typologies techniques (types d'attaque) et l'idée que n'importe qui peut être une cible ou peut dire en être l'auteur.

Toutefois, il n'y a pas vraiment de modèle qui ressort du discours. Bien que certains textes tentent d'inscrire la cyberattaque dans une perspective téléologique : la compromission de l'intégrité, la disponibilité, la confidentialité de l'information par l'accès illégitime, l'altération ou destruction. Certains auteurs ont également proposé l'idée qu'une cyberattaque allait du « virtuel vers le réel ». Cette dernière idée ne peut être validée dans le cadre de cette recherche. Une seule cyberattaque peut cibler un objectif ou des millions d'objectifs. La même cible peut être touchés par plusieurs cyberattaques. D'ailleurs, il est également possible d'être touché sans avoir été ciblé au préalable. Ceci est permis par des moyens techniques de ces attaques, qui les rendent possibles, et qui sont à la fois faciles d'accès et diffusés à grande échelle. Par ailleurs, ces attaques n'ont pas toujours des effets sensibles. Tout fonctionnement anormal d'un dispositif technique peut donc l'amener à être considéré comme faisant l'objet d'une attaque. Il existe plusieurs types d'attaques. Toutefois, certains types d'attaques reçoivent plus d'attention que d'autres :

- Les attaques par déni de service (*DoS*) qualifient l'ensemble des actions visant à mettre un serveur ou un réseau hors service. Elles sont dites « distribuée » (DDoS) lorsque l'attaquant utilise un réseau de machines tierces. La distribution permet de bénéficier d'un effet multiplicateur de l'attaque. Ce type d'attaque peut opérer en exploitant les failles d'un système, en inondant le système de requêtes selon divers protocoles, en jouant sur les failles de ces mêmes protocoles. Le principe commun est d'opérer une saturation des réseaux ou de jouer avec les limites de calcul des machines attaquées. C'est un terme générique qui peut recouvrir un large ensemble de diverses manœuvres allant de l'inondation complète d'un réseau, au blocage d'un utilisateur particulier en passant par la perturbation des connexions entre plusieurs machines. L'auteur n'a pas besoin de matériel sophistiqué.

⁷⁹⁷ Peuvent aussi se retrouver les expressions « attaque ciblée », « attaque en ligne » ou « attaque en profondeur ».

- Les virus informatiques et autres logiciels malveillants figurent souvent parmi les attaques recensées. La priorité, tout discours confondu, semble s'orienter ici vers les chevaux de trois (*Trojan horse* ou plus simplement « *Trojan* »). Ce dernier n'est pas à proprement parlé un virus, c'est un logiciel en apparence normale qui va servir de vecteur à un parasite informatique d'une autre nature (virus, logiciel espion, enregistreur de frappe, zombificateur...).
- Sont également considérés comme des attaques les campagnes de filoutage (*phishing*), des courriels contrefaits destinés à soutirer des données personnelles aux victimes qui représentent la majorité des attaques, avec les rançongiciels (*ransomware*), un programme qui chiffre une partie des données stockées sur un système et ne libère celle-ci qu'après versement d'une rançon.

L'attaque est toutefois limitée pour dépeindre l'intégralité de la cybermane. Dépendant exclusivement du moyen employé, son lien avec l'information comme cible ou les intérêts des acteurs n'est pas immédiat. Ainsi, elle ne recouvre pas directement : l'espionnage, l'ingénierie sociale, le harcèlement, le crime, la fraude, les lanceurs d'alerte, la contrefaçon, la propagande, le vol de données, les atteintes aux sites internet, les atteintes à la réputation ou aux libertés, l'usurpation d'identité... Ce sont autant de type de menaces auxquelles les utilisateurs peuvent être confrontés. En dehors des emplois, une autre typologie présente est celle de la « source » de la menace. Quel est l'élément déclencheur d'un incident en matière de sécurité de l'information. Cette approche guide notamment une grande partie des actions de prévention dans les corpus 4 et 5. Autour de l'année 2013, le discours a connu une mutation qui a questionné la place de l'élément déclencheur dans la réalisation de la menace. Nous retrouvons l'idée de l'erreur humaine commise par un individu. Ceci traduit une forte préoccupation pour l'individu qui vient un peu contredire les préoccupations du discours en matière de désignation d'un adversaire.

Le terme cyberattaque est peut-être finalement le moins spécifique des termes discutant de sécurité, car il est souvent utilisé pour désigner toute activité malveillante via le cyberspace. Comme nous l'avons vu cela inclut la propagande, le déni de service, la corruption de données, l'espionnage ou le sabotage. Les effets peuvent ou ne peuvent pas être violents et, en fait, peuvent ou ne peuvent pas se répercuter sur le monde physique. La plupart de ces activités ne seraient pas considérées comme une attaque dans les utilisations normales du terme.

La désignation de l'adversaire pose un problème dans le discours. On observe une étrange dialectique entre l'attribution de l'origine de la menace réalisée et l'auteur de la menace. L'origine de la réalisation de la menace se trouve dans le comportement fautif de la victime qu'il soit collectif ou individuel. Toutefois, celle-ci n'est paradoxalement pas l'auteur de la menace d'après le discours. En effet, la représentation de la sécurité de l'information oppose à cette vision « accidentelle » un spectre large de menaces d'origines diverses. Les acteurs sont simples à identifier. Il existerait des acteurs collectifs et individuels. Le premier acteur du discours est l'État, donc le premier acteur menaçant est un autre État. Suivent les organisations internationales, commerciales, politiques, terroristes, ou criminelles. Conscient que nous venons ainsi de désigner l'intégralité ou presque des organisations du monde social, nous renvoyons aux nombreuses typologies produites par les différents auteurs.

La diversité des acteurs appelle une première logique de désignation qui est l'indifférenciation de l'origine et des motivations de la menace. D'après le discours, la menace peut venir de n'importe où : de l'individu et à l'État en passant par entreprise commerciale ou des groupe terroriste. Elle peut cibler n'importe qui pour n'importe quelle motivation : politique, commercial, idéologique, psychologique. Quel que soit le type de menace, toutes les menaces ne se valent pas forcément, mais elles sont d'une nature fondée sur l'information. Donc, finalement la gravité de la menace ne semble pas être un critère important dans la désignation de celle-ci. La menace est invisible la plupart du temps. Ce principe a deux conséquences pour la désignation de l'adversaire : un caractère latent perpétuel qui interroge la capacité des acteurs à construire un modèle de la menace à venir, un principe de duplicité. La première conséquence vient renforcer le caractère « imprévisible » et « sous-estimé » de la menace. La seconde décrit l'existence d'une nouvelle dimension d'utilisation de l'information dans les relations de l'acteur considéré qui alimente une forme de méfiance du niveau de l'État jusqu'au niveau de l'individu. Non seulement n'importe qui peut devenir une menace, mais les relations avec des tiers peuvent également factices. Un principe d'incertitude pèse donc également sur les relations entre les acteurs.

Enfin, nous constatons dans le discours des liens entre terrorisme et sécurité de l'information, ainsi que des liens avec le crime organisé. L'observation des résultats permet de décrire une convergence des menaces autour des aspects de l'information. La cybermenace opère ainsi un point de jonction entre différentes menaces et différentes figures de l'ennemi. La menace est principalement attribuée à des adversaires classiques de l'acteur considéré.

Telle que mise en valeur au sein du discours, la définition de la menace nous permet d'établir les caractéristiques spécifiques suivantes. Ces caractéristiques sont principalement discursives et idéologiques.

La cybermenace est principalement indéterminée et indéterminable en dehors de son vecteur. Cette indétermination présente dans le discours n'est pas pathologique mais représente une composante fondamentale de la nature même de la menace de l'information. La cybermenace est ainsi caractérisée par l'ensemble des choses préjudiciables qui peuvent se produire par l'intermédiaire de l'information. Son contenu technique et pratique n'est pas fixe. De facto, elle représente une notion plus efficace que la cyberattaque pour comprendre l'ensemble des actes de nature à soulever une question de sécurité. Il est important de faire état que d'autres notions ont été proposées par les auteurs pour qualifier ces pratiques. Il y a par exemple la cyberagression⁷⁹⁸ ou le cyberconflit⁷⁹⁹. Toutefois, la cybermenace par sa définition attachée au vecteur permet de rester neutre et ouverte technologiquement. Le caractère indéterminable de la menace emporte également des conséquences pour les acteurs. Toute personne ou organisation peut en être victime ou en être à l'origine. La différence de niveau ou d'échelon entre les acteurs ne suppose pas un fonctionnement différent du discours. Toutefois, elle ne se contente pas de brouiller les différences entre les acteurs. Elle brouille également les frontières entre victime et auteur de la menace. En effet, lorsqu'elle se réalise elle peut transformer sa cible également en menace pour la sécurité dans une logique de contamination. En tant que menace indéterminable, la cybermenace est par nature latente. Elle possède un caractère imprévisible et sous-estimé.

La cybermenace procède d'une causalité multiple et transverse pouvant impliquer une part d'accident. La réalisation d'une cybermenace résulte le plus souvent d'une erreur humaine. Toutefois, le discours nous dit aussi que l'origine de la cybermenace réside dans l'intention *a priori* « malveillante » de l'auteur (distincte de la simple erreur). Même si certains hackers peuvent employer des attaques dans des objectifs en accord avec les valeurs de l'organisation cible. Ou encore, même si la recherche de protection contre les virus, suppose un travail de

⁷⁹⁸ Selon Nicolas Ténèze l'agression permet d'inclure : les attaques de déni de service, l'espionnage, le harcèlement, la fraude, les lanceurs d'alerte, la contrefaçon, le marché noir, la finance criminelle, la propagande, l'usurpation d'identité, le cambriolage de données, le « défaçage » des sites Internet. TENEZE Nicolas, *Combattre les cyberagressions*, Paris, Nuvis, Janvier 2018, 578 p.

⁷⁹⁹ VENTRE, 2011, op-cit.

production dans ce domaine. Enfin, la menace a également une composante chaotique. On peut être victime de la cybermenace en l'absence de volonté de l'auteur initial ou en l'absence d'auteur.

Enfin, la causalité multiple et traverse combiné au caractère indéterminable de la menace produisent un climat de défiance généralisé. La cybermenace produit un manque de confiance dans les relations entre les acteurs au plan international, inter-organisationnel, inter-individuel et entre ces niveaux. La cybermenace produit enfin un manque de confiance dans les relations entre les acteurs et l'objet technique. L'utilisateur n'ayant que peu de moyen de savoir si la menace se réalise ou non doit par prudence considérer une machine comme contaminée au moindre signe de dysfonctionnement. Parmi les deux hypothèses qui consistent à affirmer que la technologie est de confiance ou non. La plus simple à démontrer est qu'elle ne l'est pas. A l'inverse, la seule machine fiable est celle qui est dans l'incapacité d'exercer la moindre activité d'information.

2 – L'imaginaire victimaire et nécessité d'action : enjeux de légitimation des acteurs.

L'analyse a permis de mettre en valeur l'importance de l'échelon individuel. L'individu se comprend comme une abstraction désignant le lecteur potentiel du journal selon les perspectives éditoriales de celui-ci : l'individu connaît autant de variations que de journaux présents dans chacune des bases de données. Toutefois, cet individu possède une caractéristique commune quel que soit son type : c'est un utilisateur. Chaque individu cible a une interaction quotidienne avec un environnement numérisé où les technologies de l'information jouent un rôle considéré comme important. Du point de vue du discours, cet individu se caractérise avant tout par le fait d'être une victime en puissance⁸⁰⁰. La victimisation est en réalité au cœur du discours sur la sécurité de l'information quel que soit le niveau de dialogue que l'observateur cherche à appréhender (y compris au niveau des États et des organisations internationales). Se

⁸⁰⁰ Sur le sens du mot victime : LAMARRE Christiane, « Victime, victimes, essai sur les usages d'un mot », in GARNOT Benoît (dir.), *Les victimes, des oubliées de l'histoire ?*, Presses universitaires de Rennes, 2000, pp 31- 40. Sur la possibilité de se définir comme victime en dehors de tout lien d'infraction : FAINZANG Sylvie, *Ethnologie des anciens alcooliques*, Puf, 1998, 2e éd., 176 p. Sur l'idée de la victimisation comme contestation d'un principe méritocratie, la dialectique entre « subir » et « faire », ainsi que l'idée de concurrence des victimes, voir CHAUMONT Jean-Michel, *La concurrence des victimes : génocide, identité, reconnaissance*, La Découverte, 1997, 392 p.

présenter soi-même ou autrui comme une victime légitime l'acteur à vouloir établir des mesures protectrices sur l'information.

Concernant les acteurs des relations internationales, cette victimisation existe selon deux modes opératoires : un discours qui consiste à se présenter comme victime d'une menace de l'information et d'autre part, le fait de se défendre contre les accusations d'être une source de cybermenace contre les autres acteurs. Le phénomène du cyberspace compris par ses aspects discursifs s'insère ainsi dans une chaîne de connotations indiscutables autour de la sécurité de l'information. Cette construction de sens vient ensuite allouer l'identité des sujets de la sécurité et permet de former un cadre qui permet d'interpeller lesdits sujets. La création de ces représentations fonde l'intérêt collectif compris autour de la sécurité de l'information dans processus d'articulation/interpellation⁸⁰¹.

Tout le monde peut être victime sans distinction à partir du moment où l'on dispose d'un équipement informatique quelconque : ordinateur, téléphone portable, carte de crédit, GPS, objet connecté... Les atteintes commises par l'information ne sont pas des atteintes envers un système informatique cible de l'attaque ou envers des données mal acquises ou mal employées, mais envers l'individu. Cette victimisation repose sur un principe de représentation de complexité et une sacralisation de la machine. La machine est singulière et en dehors de la compréhension profane. L'individu est peu capable de compréhension car l'objet susceptible de connaissance est « trop technique ». Ce caractère technique (supposé) favorise le développement d'une forme de mystique autour des technologies de l'information⁸⁰². Les origines littéraires des termes « cyber » et sa difficile identification technique viennent renforcer cet aspect mystique du phénomène et les nombreuses rumeurs et récits qui se retrouvent dans les corpus presse.

Corolairement à cela, le « coupable » peut être n'importe qui : un criminel, délinquant, terroriste, hacker, bien évidemment, mais également un proche ou des communautés virtuelles (notamment dans le cadre des pratiques de cyberharcèlement ou de divulgation de contenu et

⁸⁰¹ Termes employés pour décrire le concept d'intérêt national. WELDES Jutta, « Constructing National Interests », *European Journal of International Relations*, 2 (3), 1996, pp. 280 à 289.

⁸⁰² Sur l'exagération des représentations de l'informatique, voir en particulier PAVE Francis, *L'illusion informaticienne*, Paris, L'Harmattan, 1989, 270 p. ; voir également FIALAIRE Jacques. « L'évolution des politiques d'informatisation de l'administration publique en France. Quelles articulations entre services centraux et déconcentrés de l'État ? », *Politiques et management public*, vol. 10, n° 4, 1992. pp. 55-63.

de données personnelles). Si la victime peut être tout le monde, il en va ainsi de même pour l'auteur de l'attaque. Les premiers coupables ciblés par le discours sont paradoxalement les victimes elles-mêmes, coupables d'imprudence et/ou d'absence de maîtrise des technologies de l'information au travers d'un usage déraisonnable ou par naïveté. C'est enfin la trop grande dépendance de la société qui est montrée du doigts comme un vecteur d'insécurité.

En résumé, le discours de sécurité tel qu'il ressort de notre analyse repose sur deux principes : la menace est imprévisible et irrésistible. L'acteur-utilisateur existe comme une victime potentielle de tout le monde y compris de lui-même à travers l'informatique, et il n'a aucun moyen d'assurer sa propre sécurité de manière autonome. Ce discours de sécurité s'appuie également sur une représentation technique et mystique des technologies de l'information.

Paradoxalement, cette idée victimale ne participe pas qu'à décrire un besoin de sécurité mais justifie également un important besoin d'accès aux technologies de l'information, également fondé sur l'idée d'une maîtrise imparfaite et de l'insuffisance de leur diffusion pour répondre à l'ensemble des besoins qu'elles ont vocation à couvrir. Il n'est donc pas illogique de constater que les termes qui se dotent du « label » cyber (notamment dans les groupes « autres ») servent à évoquer l'enjeu des technologies de l'information propre à chacun des secteurs concernés (agriculture, tourisme, environnement, santé, robotique...). Contrairement aux discours institutionnels, il n'y aurait non pas un unique besoin de sécurité mais un besoin de technologies de l'information majoritairement doté d'un aspect sécuritaire face auquel l'acteur est démunie et qui justifie une réponse par le commerce ou les institutions.

Une exception à cette victimisation relève de la négligence coupable quand l'acteur est réputé avoir un devoir en matière de sécurité de l'information. En effet, quand bien même l'acteur n'aurait pas été victime d'une atteinte par le biais de l'information, il sera alors coupable de négligence. Autrement, il n'en aura pas « fait assez » contre la menace. Il y a donc également une rhétorique de la nécessité de l'action qui rentre en ligne de compte.

La victimisation se traduit selon trois postures qui visent à reconnaître l'existence d'une victime : se déclarer soi-même victime « Les intérêts que je juge miens sont menacés », déclarer autrui victime « Les intérêts d'autrui sont menacés », et se déclarer victime d'une accusation « Je suis (falsement) accusé d'être une menace pour les intérêts d'autrui ». Se déclarer soi-même comme victime, permet d'assurer une forme de défense légitime que constitue les

politiques et moyens exceptionnels alloués à la gestion du risque et de la menace informatique. Déclarer autrui menacé permet de légitimer une forme d'intervention à son profit (de la prévention à la protection). Se défendre d'accusation l'accusation d'être une menace permet de conserver le statut de victime.

Ce statut social est particulièrement précieux. Dans un discours qui admet tout le monde comme une victime en puissance du particulier à l'État, il n'y a que deux possibilités : être dans le camp des victimes ou non. Si la menace peut être caractérisée comme de relative faible importance quantitative, cela ne pose pas de soucis. La particularité du cyberspace c'est qu'il est dépeint comme une figure de la menace totale allant de la petite criminalité aux opérations militaires en passant par l'intégration de certaines composantes environnementales (l'effondrement du système). Toute activité susceptible de numérisation entre dans la métaphore. Le discours n'est pas suffisamment structuré pour établir clairement de distinction. Le menace de divulgation de données personnelles et/ou privées existe dans la même représentation que les images de propagande terroriste ou encore que les opérations militaires visant à paralyser les communications d'un ennemi : tout cela fait partie de la cybermenace. Face à un discours si terrible, il est important de préserver cette image de victime pour l'acteur des relations internationales lorsque la défense de ses intérêts ou des intérêts d'autrui ne justifie plus des moyens exorbitants du droit commun pour les protéger. Dans ce domaine particulier, les États qui font le plus d'efforts pour se présenter sous un jour positif sont : les États-Unis d'Amérique, la Chine, la Russie... Toutefois, cette pratique s'étend à toute organisation susceptible d'être accusée (y compris des sociétés privées). D'un point de vue caricatural, nous pourrons affirmer que l'une des expressions de la force en matière d'information numérisée consiste à tenter de préserver son statut de victime afin de conserver une forme de légitimité politique.

B – Des éléments concrets de la menace : la dépendance à l'information.

Le discours mobilise l'idée de dépendance principalement pour décrire un état de trouble affectant l'individu. Le lexique produit parle notamment de cyberdépendance ou de cyberaddiction. Les dérivés du cyberspace ne sont pas les seuls termes employés pour décrire ce qui est nommé comme un trouble d'usage, comportemental. Cette dépendance se cristallise sur un objet particulier : Internet, jeux vidéo, pornographie, smartphones, réseaux sociaux... Cette thématique est principalement issue des travaux de recherche en psychiatrie et en

psychologie. L'idée de cyberdépendance trouve une seconde application : celle de la dépendance des organisations aux technologies de l'information.

Cette seconde dépendance existe à trois niveaux discours différents : la dépendance de l'acteur aux systèmes d'information, la dépendance des systèmes à des acteurs extérieurs à l'acteur de référence, et enfin la dépendance des systèmes entre eux. Elle est toujours présentée de manière systémique (au sens large) et croissante. Elle est principalement présentée en miroir de la résilience (corpus 3), elle peut l'être de façon minoritaire avec l'idée de sécurité (assez rarement dans les corpus 3, 4 et 5). Cette dépendance se fonde majoritairement sur les ressources. Le concept de dépendance aux ressources⁸⁰³ illustre un modèle d'organisation où la survie est dictée par les contraintes propres à son environnement⁸⁰⁴.

La dépendance aux systèmes d'information traduit une dépendance aux ressources qui vient affecter le comportement de l'acteur-utilisateur. Ce premier cas met en avant l'idée de paralysie de l'acteur en cas d'incident. Il ne peut pas être acteur s'il ne dispose plus de l'utilisation du système. L'acteur doit se doter d'un système d'information. L'utilisation d'un système d'information confère la qualité d'acteur. Cette dépendance alimente ainsi l'ontologie de la résilience qui vise une continuité de l'acteur y compris en cas d'incident (donc une relative absence de paralysie du fait d'une indépendance du système).

La dépendance de l'acteur à des acteurs extérieurs au travers du système vise l'absence d'autonomie du premier au profit des seconds. Elle est aussi une forme de dépendance aux ressources. Le lien de dépendance entre l'acteur et son système d'information entraîne une dépendance aux acteurs extérieurs dont il a besoin pour concevoir, construire, maintenir et faire fonctionner ce système. Il s'agit d'une dépendance aux fournisseurs de matériels et de services : des machines aux logiciels. Le discours intègre cette idée pour décrire une nécessité de développement de la sécurité, mais également pour traiter des questions commerciales et de concurrence. La dépendance peut notamment être utilisée pour décrire une situation avantageuse sur le marché (« dépendance aux Fournisseurs d'accès Internet », « dépendance

⁸⁰³ Principalement théorisée à partir de 1978 par Jeffrey Pfeffer et Gerald Salancik, elle est intégrée aux théories de la contingence en sociologie des organisations. PFEFFER Jeffrey et SALANCIK Gerald, *The External Control of Organizations*, New York, Harper & Row, 1978.

⁸⁰⁴ CROZIER Michel et FRIEDBERG Erhard, (1977). *L'acteur et le système : les contraintes de l'action collective*. Coll. « Points Essais ». Paris, Éditions du Seuil, 2014, 512 p.

aux géants du web ou aux « GAFA »⁸⁰⁵ ...), mais également des situations de dépendance entre États. La dépendance entre États touche principalement aux infrastructures, aux ressources (terres rares, composants) et également aux logiciels.

L'interdépendance systèmes caractérise un degré de complexité de la ressource. Un élément de donnée ou agent logiciel peut avoir besoin d'un autre élément pour fonctionner. La dépendance est un volet de l'interconnexion qui caractérise le cyberspace dans la plupart de ses définitions. Toutefois cette dépendance n'est pas que technique, mais résulte en partie du rôle et de l'utilisation de la technologique pour l'acteur qui peut employer plusieurs outils dans le cadre de son activité. A une échelle toujours bien différente de celles des relations internationales, un exemple d'une situation de dépendance pourrait être la mobilisation de différents outils rendue nécessaire par une question propre à l'acteur alors que les outils n'ont pas de lien technique entre eux. En guise d'exemple, prenons un établissement de formation qui construirait ses emplois du temps (sur un logiciel acheté auprès d'un prestataire) établis en fonction d'un programme de formation (sur un logiciel propriétaire) lui-même établi en fonction d'un plan de formation (sur un tableur type Microsoft Excel). Vouloir supprimer le logiciel intermédiaire pourrait conduire la paralysie de toute l'opération de construction des emplois du temps, du seul fait de l'organisation. Cette paralysie pourrait être décrite comme une dépendance particulière de l'acteur à son système d'information et un manque de résilience.

La dépendance à l'information caractérise ainsi une forme de dépendance à des ressources complexes potentiellement interdépendantes, et aux travers de ces ressources à des tiers fournisseurs de bien et de services. Le modèle de la dépendance aux ressources suppose un environnement incertain. En tant que discours, la cybermenace vient renforcer cette incertitude. Autrement dit, un acteur sera d'autant plus sensible à la cybermenace qu'il sera dépendant à l'information. La résilience constitue ainsi la recherche d'indépendance et de réduction de cette incertitude. Le positionnement de cette dépendance ne se situe pas dans un espace métaphorique abstrait. Au contraire, il passe par la mise en question concrète des rapports entre l'information et l'acteur dans toutes leurs composantes à la fois aux plans techniques et aux plans humains.

⁸⁰⁵ Acronyme de Google, Apple, Facebook et Amazon

La dépendance n'est toutefois pas un thème majeur du discours (outre la dépendance psychologique des individus). Les corpus analysés insistent beaucoup sur la menace sans insister sur ce dernier thème. Elle revêt pourtant un caractère fondamental du point de vue de la compréhension de la menace : Qu'importerait une menace qui n'aurait pas d'impact pour la sécurité des acteurs ? Serait-elle encore une menace ? Les mesures exceptionnelles qu'elle implique seraient-elles toujours perçues comme légitimes ? Si la dépendance n'est que peu promue par le discours, c'est sans doute car elle impose une compréhension critique pour justifier une mesure. Elle est connotée négativement. De plus l'idée de dépendance va contre trois fonctions importantes du discours analysé : la description de la menace, la désignation d'adversaire et la victimisation. La dépendance à l'information propose une nouvelle description de la menace différente de la cybermenace. Elle suppose une démarche interne et ne se préoccupe que peu de l'adversaire. Comme nous l'explique la cyberdépendance, être dépendant, c'est avoir une maladie. Dire la dépendance c'est admettre que quelque chose ne va pas dans le mode de fonctionnement que l'on essaye de préserver, donc aller contre le discours de sécurité. Enfin, une victime consciente de l'étendue exacte de sa vulnérabilité serait « moins légitime » qu'une victime totalement démunie et passive, du fait de la diminution de la menace opérée par elle.

C – Valorisation et capitalisation de l'information : de l'inégalité des acteurs en termes d'information.

Face à la cybermenace totale, le discours oppose une stratégie spécifique. Cette stratégie de protection repose principalement sur le développement et la mise en avant de la connaissance comme forme particulière de l'information. Elle découle d'une volonté de retrouver la maîtrise de l'information face à une menace transversale, opaque et dynamique. L'information constitue le levier autour duquel se construit le sens de cette culture. Cela est marqué par le vocabulaire dans l'attribution de connotation plus ou moins positives aux langages servant la représentation (par l'opposition : cyber, péjoratif / numérique, mélioratif).

La valorisation s'entendra ici comme une mise en valeur positive de la connaissance. Cette posture intègre plusieurs dimensions. Le premier niveau de valorisation de cette connaissance réside dans l'importance accordée à la formation. Cette formation passe par l'éducation, la prévention, la formation des utilisateurs, la formation des spécialistes. De nombreuses publications comprises au sein des corpus insistent sur cette dimension.

L'ensemble de ces activités de formation insistent sur la prise de conscience et le transfert de compétences utiles pour maîtriser l'information et prévenir la menace. Dans ce contexte, ce n'est pas seulement l'image des réseaux, des flux qui domine la représentation mais aussi celle du savoir, de l'expertise ou encore de l'innovation voire de la créativité à opposer à la menace totale.

La prévention est mobilisée de manière générale pour insister sur l'un ou l'autre des enjeux et n'a pas de domaine spécifique. L'éducation est plutôt mobilisée sur les thématiques de cyberharcèlement, de prévention de la criminalité, de la pédophilie, de la dépendance et de la violence de certains contenus (ou tout simplement pour dire que les téléphones personnels des apprenants sont interdits au sein des établissements de formation). L'éducation se destine prioritairement à un public « familial » (parents/enfants) ou des professionnels du domaine de l'éducation. La formation des utilisateurs est principalement utilisée dans un contexte professionnel et/ou contre les cybercriminels et les pratiques qui leur sont associées (Même s'il serait plus opportun de parler de « pratique cybercriminelle », la criminalité organisée qui est sous-entendue lorsque la cybercriminalité n'étant qu'une catégorie d'auteurs desdites infractions). La formation des spécialistes concerne principalement la sécurité des systèmes et consiste le plus souvent à pointer un besoin (plutôt les corpus 1 à 3) ou à mettre en valeur la création d'une formation diplômante spécifiquement dédiée (tout corpus). Ces deux dernières thématiques sont plus présentes dans les discours institutionnels.

Outre cette importance de la formation, le discours fait également une place importante à la production de connaissance à travers la valorisation de la recherche académique mais également par le soutien d'un grand nombre de publications consacrées à cette question du cyberspace. Toutefois, ce niveau de publication ne saurait égaler l'ensemble des activités de communication à caractère plus ou moins académique qui entourent le discours sur la sécurité de l'information. On ne compte plus depuis quelques années, le nombre de « colloques », conférences, challenges, concours, création de chaire sur la base du mécénat, qui ont ouvert sur cette question. Cette dimension particulière de la recherche fera l'objet du prochain chapitre mais elle participe également d'une mise en valeur de la connaissance par le discours.

Enfin, la valorisation de la connaissance passe également par une forme de partage de celle-ci. Une importance est accordée dans le discours à certains outils de médiation et de partage du savoir ainsi que l'accès à l'information. L'accès à l'information est d'abord

représenté comme un accès social à la culture et à la technologie. Ce rapport structure en partie l'idée de détenir de la connaissance dans une perspective individualiste entraînera une représentation « négative » de l'acteur. Tandis que le partage de ces informations sera perçu de manière « positive ».

La valorisation de la connaissance participe à la diffusion en dehors des appareils de l'acteur régional d'une « culture de renseignement », laquelle devient alors accessible au plus grand nombre⁸⁰⁶. Cette culture politique de renseignement ne s'entend donc pas au sens « culture politique institutionnelle ». En effet, d'un point de vue académique, la notion de « culture du renseignement » (institutionnelle) est majoritairement utilisée dans les approches comparatives ou critiques sur l'organisation et la place des services de renseignement au sein d'un État donné. Autrement dit, la notion de culture du renseignement décrit une forme de rapport qu'entretient une collectivité nationale avec le renseignement institutionnel⁸⁰⁷. Parler de culture « de » renseignement opère une ouverture du concept vers son sens fonctionnel. Dans un contexte vague et incertain, où l'information n'est disponible que de manière limitée⁸⁰⁸, cette culture traduit la préoccupation de maintenir un niveau de connaissance utile à la prise de décision : autrement dit, d'avoir une activité de renseignement. « Le renseignement se distingue de l'information, non par sa nature (objet, origine, moyens de recueil, traitement), mais par sa finalité (l'utilisateur) qui le caractérise entièrement. »⁸⁰⁹.

Jean-Claude Passeron fait de la culture un des concepts polymorphes, marqués par la multiplicité des emplois descriptifs dont ils ont été l'objet⁸¹⁰. La culture d'un groupe opère selon trois grandes catégories de sens qui décrivent l'ensemble de sa morphologie : style de vie,

⁸⁰⁶ Sur le renseignement en général et ses domaines, voir notamment : SOUTOU Georges-Henri. « La stratégie du renseignement : essai de typologie », *Stratégique*, vol. 105, no. 1, 2014, pp. 23-42.

⁸⁰⁷ DENECE Éric, ARBOIT Gérard, « Les études sur le renseignement en France », *Rapport de Recherche* n° 8, Centre Français de Recherche sur le Renseignement, Novembre 2009, p. 21

⁸⁰⁸ Sur la place de la rationalité dans les Relations Internationales, voir : ALLISON Graham T. et ZELIKOW, Philip, D., *Essence of Decision: Explaining the Cuban Missile Crisis*, 2^{ème} édition, Longman, 1999. Ainsi que les deux numéros de la revue *Culture et conflits* : « Rationalités et Relations Internationales », vol. 1 et 2, n°36 et 37, hiver 1999 - printemps 2000. Et notamment, HAINE Jean-Yves, « Rationalités et relations internationales : l'inaccessible synthèse ? », *Cultures & Conflits*, 36, hiver 1999 - printemps 2000.

⁸⁰⁹ BEAU Francis, « Culture du renseignement et théories de la connaissance », *Revue internationale d'intelligence économique*, vol. vol 2, no. 1, 2010, pp. 161-190. Voir également : BULINGE Franck, et BOUTIN Éric. « Le renseignement comme objet de recherche en SHS : le rôle central des SIC », *Communication & Organisation*, vol. 47, no. 1, 2015, pp. 179-195.

⁸¹⁰ PASSERON, *Le raisonnement sociologique*, op-cit p. 36 et p.445. Le concept de culture est surtout utilisé chez Passeron pour décrire l'action culturelle.

comportement déclaratif (idéologies) et corpus d'œuvres valorisées. La culture peut donc s'entendre comme l'ensemble des modèles de représentations et de pratique qui régularisent, en ajoutant leurs effets, l'usage des technologies matérielles, l'organisation des moments de la vie sociale, des catégories de pensées ou du sentiment d'appartenance. Passeron décrit le style de vie comme doté d'une grande capacité d'absorption des apports extérieurs qui maintient son existence dans la durée. La culture peut également s'entendre du discours oral ou écrit médiatisée par un langage. Cet aspect est celui qui évolue le plus vite. Enfin, le corpus d'œuvres valorisé comprend principalement les faits culturels mis en avant par le groupe social étudié de même que les faits écartés par celui-ci.

Du point de vue de cette conception de la culture, parler de renseignement revient donc à cerner découvrir des composantes qui sont autant de sens possibles : un « style de vie », un « comportement déclaratif » et « des œuvres valorisées ». Du point de vue, du style de vie, une culture de renseignement désigne une posture de recherche d'information aux fins de prise de décision. Les faits sociaux valorisés par cette culture sont conférés par l'utilité du renseignement obtenu dont le degré de pertinence détermine la valeur. L'œuvre est le « document », soit l'enregistrement d'un « savoir ». Ce savoir se comprend ici comme une valorisation de l'information comme représentation de la réalité (faits). Cette information subit un processus de transformation visant sa mémorisation par une double logique de lecture (perception / acquisition / appropriation) puis de restituée sous la forme d'une donnée exploitable pour la prise de décision⁸¹¹. Dans ce modèle de pensée, le document est le « véhicule universel de la connaissance et des savoirs » dans un système d'information donné⁸¹². La numérisation du document replace la nécessité de l'humain au cœur du dispositif d'intelligence en lieu de place de la machine. Sous le paradigme du renseignement, le système d'information met en valeur l'organisation du jeu collectif et au travail d'équipe en réseau qu'aux performances techniques des outils.

Le caractère déclaratif de la culture nous permet ici d'établir un lien avec le discours. Le discours qui entoure le renseignement se voit souvent reprocher une forme de confusion et d'imprécision. L'idée de culture de renseignement semble ainsi faire bénéfice d'un ensemble discursif dont le cyberespace n'est finalement qu'une composante. En témoigne la popularité

⁸¹¹ BEAU Francis, 2010, op-cit. §73.

⁸¹² Ibid, §87 et §91.

de nombreux termes et expressions autour de l'information : intelligence économique, espionnage industriel, renseignement économique, financier, de sécurité, criminel, politique, ou encore l'ingénierie sociale. De plus, le cyberspace opère une forme de substitution de certains de ces termes pour s'étendre hors de la seule sécurité des systèmes. C'est notamment le cas avec l'intelligence économique, laquelle est supplantée par la cybersécurité comme thématique à la mode à la fois dans les journaux, mais également du point de vue de l'ouverture de formations et de créations d'entreprise.

La capacité à produire et détenir de l'information permet de créer et de valoriser un ensemble de systèmes sociotechniques dédiés à la prise de décision. Lesquels forment le gros des œuvres culturelles associés à ce discours de sécurité. D'un point de vue militaire sur les questions de sécurité de l'information, une œuvre de ce type peut être caractérisée en France notamment sur des dispositifs tels la *Recognized Cyber Picture* dans l'armée de l'air (RCP Air) fondée dans la continuité de la *Recognized Air Picture* (RAP) comme une représentation pertinente et opérationnelle des situations d'intérêt pour le système de force et les opérations dans lesquelles il se déploie⁸¹³... La logique est la même concernant l'importance accordée plus généralement dans tous les États de l'OTAN aux systèmes de *command and control* (C2)⁸¹⁴ et toutes leurs variantes⁸¹⁵, présent dans les travaux de recherche militaire notamment américains. Si on prend de la hauteur par rapport à la technique et la pléthore des acronymes, le développement de ces systèmes représente bien une diffusion d'une culture de l'information particulière articulée autour de la finalité de la décision. Ce développement représente une intégration dans tous les aspects de la vie d'une organisation d'une culture de renseignement articulée autour de la représentation de « guerre réseau-centrée » (*Network centric warfare*, NCW). Culture de renseignement et valorisation de l'information aboutissent à des situations d'inégalité du capital informationnel détenu par un acteur donné. D'où, une production de

⁸¹³ BARBAROUX Pierre, « Cyberdéfense et cybersécurité du milieu aérospatial : quelles spécificités ? quelles ambitions ? », *Penser les ailles françaises*, n°32, juillet 2015 pp. 89 – 96.

⁸¹⁴ VASSILIOU Marius, ALBERTS David S., et AGRE Jonathan R, *C2 Re-Envisioned: the Future of the Enterprise*, CRC Press, New York, déc. 2014, 316 p.

⁸¹⁵ Ces variantes dépendent pour beaucoup des auteurs et ont grandement varié au cours du temps. Ainsi chez les américains, l'actuel acronyme DoDAF (*Department of Defense Architectural Framework*) s'est vu implanté du C4ISR (*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*, lequel dernier était parfois remplacé par *Target Acquisition and Reconnaissance*). Ce C4ISR représentant lui-même une évolution selon une longue chaîne d'acronymes depuis le « C2 » dont voici quelques exemples : *Command, control, and communications* (C3); *command, control, and communication system* (C3 system); *command, control, communications, and computers* (C4); *command, control, communications, and intelligence* (C31); et *command, control, communications, intelligence, and interoperability* (C312).

modèles tournées vers la décision par l'information, laquelle apparaît comme une tendance lourde au-delà du seul phénomène linguistique analysé.

Section 2 – Théories pour une approche discursive du cyberespace et de la sécurité de l'information.

A partir de notre analyse du phénomène et de l'observation empirique, le cyberespace et ses termes dérivés nous a semblé relever d'un discours de sécurité. Autrement dit, il s'agit de considérer que ce phénomène du langage est un artefact qui opère la transformation de l'information en enjeu de sécurité. Comprendre la sécurité en tant que discours avec une structure rhétorique et un effet politique particuliers rend le concept de « sécurisation » particulièrement adapté à une étude de la formation et de l'évolution du discours sur la cybersécurité. En effet, en établissant un lien entre la sécurité de l'information et la sécurité nationale à l'aide du phénomène linguistique « cyber », de nombreux États ont vu émerger un nouveau discours dans lequel les personnes concernées par la sécurité numérique identifient une grande variété de problèmes complexes de sécurité de l'information qui justifient un ensemble de politiques extraordinaires⁸¹⁶.

Nous retrouverons la mise en valeur de la vulnérabilité critique d'un objet de référence (information), par une construction contextualisée d'un réseau cohérent d'implications auprès d'une audience par des pratiques discursives où le langage « cyber » joue le rôle de certains artefacts heuristiques⁸¹⁷. Le propos ne vise donc plus à analyser un phénomène du langage mais à comprendre la portée, l'impact et le sens de la transformation en enjeu de sécurité de l'objet de référence que vise l'emploi de ces artefacts heuristiques.

Le point de départ pour commencer à faire le lien entre le discours et l'enjeu de l'information consiste à mobiliser la théorie de la sécurisation. Nous opterons ici pour l'approche « classique » de la cybersécurité par la sécurisation de Lene Hansen et de Helen Nissenbaum⁸¹⁸. Construite autour de l'idée d'autonomie du discours, cette section traite d'une

⁸¹⁶ Cf. première partie.

⁸¹⁷ Cf. chapitre liminaire.

⁸¹⁸ Selon Myriam Dunn Cavelty, cette approche correspond au deuxième texte le plus cité parmi les textes traitant de cybersécurité dans les Relations Internationales après l'article de Thomas Rid, (RID Thomas, 2011, op-cit) ;

part de l'application de la théorie de la sécurisation à ce dernier, avant de la confronter aux limites du phénomènes discursif et de chercher à recontextualiser la sécurité de l'information au-delà du seul phénomène « cyber ».

A – L'impact de la sécurisation : la cybersécurité comme secteur autonome ?

S'inscrivant dans la perspective de l'Ecole de Copenhague, Lene Hansen et Helen Nissenbaum ont cherché à appliquer le concept de sécurisation à la cybersécurité. Leurs travaux ont fait l'objet d'une publication en 2009⁸¹⁹. L'article repose principalement sur la comparaison entre les normes américaines et une étude de cas focalisée sur les événements estoniens de 2007 que nous rappelons en introduction du présent manuscrit. Dans la perspective de cet article, le discours sur la cybersécurité se déplace de manière transparente parmi les distinctions normalement jugées cruciales pour les études de sécurité entre sécurité sociale et collective, entre pouvoirs publics et institutions privées, et entre la sécurité économique et politico-militaire.

S'appuyant sur l'idée d'une résolution individuelle et collective, l'acteur régional implique le secteur privé comme coresponsable de la cybersécurité et le discours sur les libertés civiles vient contrebalancer cette responsabilité en exprimant la différence entre les sphères publiques et privées.

Même si elle demeure classique au sens de l'école de Copenhague, l'approche défendue par Lene Hansen et Helen Nissenbaum tient compte de l'éclatement de la sécurité entre le public et le privé, tout en actant l'idée d'une finalité commune entre ces acteurs. Pour expliquer ce

CAVELTY Myriam Dunn , « Cybersecurity Research Meets Science and Technology Studies », *Politics and Governance*, Volume 6, Issue 2, juin 2018, pp. 22-30.

⁸¹⁹ HANSEN Lene et NISSENBAUM Helen, « Digital Disaster, Cyber Security, and the Copenhagen School », *International Studies Quarterly*, vol. 53, 2009, pp. 1155–1175. Le contenu de cet article repose sur certaines publications antérieures des auteures, en particulier du côté d'Helen Nissenbaum qui a auparavant travaillé sur le phénomène des hackers depuis le milieu des années 90 et qui avant la publication de l'article objet de cette note avait publié une comparaison entre la sécurité nationale et la propriété intellectuelle sur la base du même concept de sécurisation. NISSENBAUM Helen « Where Computer Security Meets National Security ». *Ethics and Information Technology*, vol. 7, n° 2, 2005, pp. 61–73.

paradoxe, l'article fait appel à la théorie de la compétition entre l'État et le secteur privé⁸²⁰, ainsi qu'à la théorie de la multi-discursivité de la cybersécurité⁸²¹.

C'est la raison pour laquelle, nous examinerons cette théorie à l'aide de notre travail sur le phénomène proprement dit. Pour rappel, dans la conception que nous retenons des critiques adressées à l'Ecole de Copenhague, la dimension discursive se double de pratiques non discursives englobant tant les enjeux de pouvoir que les enjeux scientifiques et technologiques. Ce n'est pas la direction que les auteures ont choisi d'emprunter à ce stade de leur réflexion : celle-ci se concentrera uniquement sur l'aspect discursif. Telle qu'elle se trouve formulée, cette théorie ne permet pas de comprendre les éléments relatifs à l'émetteur du discours. L'article aboutit à la distinction de la cybersécurité comme secteur autonome⁸²² doté de ses propres objets référents et produisant une grammaire spécifique. Autant le dire tout de suite, s'il s'agit d'une approche intéressante pour comprendre le mécanisme de sécurisation et sa manière de fonctionner avec ses différentes implications politiques. Dans le but de comprendre ces mécanismes que l'article qualifiera de « grammaires », les auteures mobiliseront la typologie des discours consacrés à la sécurité et à Internet établie par Ronald Deibert en 2002.

1 – La pluralité des discours sur Internet et objets référents : la typologie de Deibert.

Ronald Deibert exploite l'idée selon laquelle plusieurs discours existent en compétition dans la cybersécurité. Cette compétition étend la constellation d'objets référents-menaces⁸²³ et

⁸²⁰ SACO Diana. « Colonizing Cyberspace: National Security and the Internet », In. WELDES Jutta, LAFFEY Mark, GUSTERSON Hugh et DUVALL Raymond (eds). *Cultures of Insecurity: States, Communities, and the Production of Danger*, Minneapolis: University of Minnesota Press, 1999, pp. 261-292.

⁸²¹ DEIBERT Ronald J. « Circuits of Power: Security in the Internet Environment » In. ROSENAU James N., et SINGH J. P. (eds). *Information Technologies and Global Politics: the Changing Scope of Power and Governance*. State University of New York, 2002, pp. 115 à 142. Voir également les articles postérieurs en particulier celui plus récent coécrit avec Rafal Rozohinski : « Risking Security: Policies and Paradoxes of Cyberspace Security », *International Political Sociology* vol. 4, n° 1 pp. 15 - 32, 2010 ; ainsi que DEIBERT Ronald J., « Black Code: Censorship, Surveillance, and the Militarization of Cyberspace », *Millennium*, vol. 32. n°33, décembre 2003, pp. 501-530

⁸²² Voir le concept des cinq secteurs de la sécurité étatique et la sécurité sociétale dans notre chapitre liminaire. En particulier : BUZAN Barry, WÆVER Ole et WILDE (DE) Jaap, 1998, op-cit.

⁸²³ « *threat-referent object constellation* ». L'auteur mobilise ici le concept de constellation en tant que constellation de sécurité. MCSWEENEY Bill, 1999 op-cit, Pour un autre exemple de l'usage du concept de constellation en études de sécurité avec le concept de securitization, voir notamment l'article plus récent : BUZAN Barry, et WÆVER Ole « Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory. » *Review of International Studies*, vol. 35, no. 2, 2009, pp. 253–276.

complexifie l'étude de ces discours. Il ajoute que les conditions matérielles de l'environnement de communication détermineront le discours dominant (ce qui se rapproche à l'échelle de cette recherche des éléments d'influence de la communauté épistémiques que nous mettions en avant). Toutefois, cela ne résout pas la question de savoir quels sont ces discours. Ces discours sont à l'époque des discours sur Internet en tant qu'artefact technique. Ronald Deibert en identifie quatre, avec des objets de référence distincts, des menaces, des choix de politique et des visions différentes de l'ordre mondial : la sécurité nationale, la sécurité de l'État, la sécurité privée et la sécurité du réseau. Il est important de souligner que cette typologie se limite à Internet, mais qu'elle constitue la base par laquelle Lene Hansen et Helen Nissenbaum examinent les discours liés à la cybersécurité.

La sécurité nationale est concernée par Internet du fait principalement du glissement de l'encadrement des normes de la radio et de la télévision vers un nouvel artefact dépourvus de l'ancienne ressource des fréquences et des chaines et pour lesquels les anciens modes de régulation ne sont plus adaptés. Internet s'inscrit dans un phénomène de globalisation que l'acteur régional cherchera à contrecarrer afin de protéger sa culture et son identité⁸²⁴. La principale menace que représente Internet est son potentiel de saper les identités nationales collectives. L'objet principal de la sécurité est présumé être « la nation » entendue comme la communauté imaginée de personnes partageant une langue ou une ethnie distincte. La réponse à cette menace varie énormément de la censure de ce mode de communication à la production d'un contenu spécifique dédié. Dans un autre registre, l'auteur pointe la possibilité d'alliances peuvent se nouer entre différents États afin de défendre leurs intérêts communs.

La sécurité de l'État est une catégorie de représentation d'Internet qui pointe directement les menaces contre la souveraineté que celles-ci proviennent de l'étranger ou ne menacent l'équilibre de l'ordre interne de l'État⁸²⁵. Deux craintes principales sont mises en avant dans ce modèle : la transformation de la guerre et la limitation du pouvoir grâce à Internet. Ici, l'artefact facilite de nouvelles formes de guerre et de violence non traditionnelles, en particulier de la part d'acteurs non étatiques et de terroristes. Une menace connexe est la perte potentielle du contrôle de l'État sur les flux d'informations entrant et sortant du pays. L'objet principal de la sécurité est l'État ou le gouvernement territorial. Les réponses politiques vont des tentatives de créer

⁸²⁴ DEIBERT, 2002, op-cit, p. 119.

⁸²⁵ Ibid. p 122

des pares-feux nationaux aux pressions exercées sur les fournisseurs de services Internet et les citoyens pour restreindre leur accès à l'information et sa diffusion, ainsi qu'à la promotion des technologies de cryptage.

La sécurité privée concerne davantage les individus. En effet, Internet y constitue une menace pour l'invasion potentielle de la vie privée par les États et les entreprises. L'objet principal de la sécurité est l'individu. Les réponses politiques issues de cette image collective incluent des règles strictes en matière de protection de la vie privée et des règles protégeant les données personnelles et imposant des restrictions quant à la manière dont ces données peuvent être utilisées, ainsi que la réglementation des technologies de cryptage. L'ordre mondial promu par cette image collective est un système d'États libéraux constitué sur la base de droits de l'homme et de protections individuelles de la vie privée.

La sécurité du réseau vient traduire pour l'auteur l'importance croissante des technologies de l'information pour tous les aspects de l'économie et de la finance. Cette sécurité du réseau est centrée sur la protection de l'intégrité des données et du flux d'informations interne à des entreprises ainsi que sur la sécurité des flux d'informations entre producteurs et consommateurs. Le réseau est l'objet-référent de la sécurité car il garantit l'intégrité de l'information. Il est matérialisé par les flux d'information et par les données numériques. La portée du réseau dépasse pour la grande partie le territoire. Ainsi les délibérations politiques qui le concernent se concentrent dans plusieurs juridictions nationales et impliquent nécessairement des alliances entre États pour aboutir. Les menaces à la sécurité du réseau incluent un large éventail d'activités qui vont des erreurs, aux accidents ou aux utilisations malveillantes du réseau.

Bien que cette typologie soit un peu vieillie du fait d'avoir été produite en 2002 et qu'elle n'emploie que peu le langage « cyber », on y retrouve des types d'images auxquelles nous avons été confrontés tout au long de cette recherche. En tant que telle, elle peut servir à rendre cohérente certaines postures et de pallier à certaines incompréhensions entre les différents acteurs. Par ailleurs, elle permet d'expliquer certaines divisions de concepts dans le discours. La critique de Lene Hansen et Helen Nissenbaum à cette typologie repose justement sur cette conceptualisation des objets de références séparés à laquelle elles préfèrent une théorie qui visent à mettre en lumière les articulations concurrentes entre les différents registres de discours

de nature à mieux rendre l'aspect dynamique (sinon parfois un peu chaotique) du terrain. Si la typologie a le mérite de clarté, ce n'est nécessairement le cas de l'empirie où les frontières n'apparaissent pas de manière si nette.

2 – Les « grammaires » de la cybersécurité : l'hypersécuritisation, les pratiques quotidiennes de sécurité et les technifications.

Partant du principe que la contestation et multidiscursivité se retrouvent à la fois entre les articulations concurrentes des objets référents ainsi que dans l'instabilité interne potentielle de chaque discours, Lene Hansen et Helen Nissenbaum propose une conception du secteur de la cybersécurité comme secteur autonome dotés de trois modalités spécifiques : l'hypersécuritisation, les pratiques quotidiennes de sécurité et les technifications.

L'hypersécuritisation⁸²⁶ se définit comme la tendance à exagérer les menaces existantes et à recourir à contre-mesures excessives. Abandonnant le caractère « exagéré » des menaces, les auteures préfèrent ici s'intéresser à l'excès dans la contremesure. En effet, le discours sur la cybersécurité repose sur des scénarios catastrophes multidimensionnels comportant une liste de menaces graves. Ces scénarios sont notamment caractérisés par deux éléments : ils opèrent selon un séquençage en cascade et aucun de ces scénarios n'a jusqu'à présent eu lieu⁸²⁷. De la simple hypothèse de l'aléa qui conditionne la réalisation de la menace, l'hypersecuritisation entraîne un effet global. La réalisation de la menace affectant l'objet-référent, n'est plus seulement limité à celui-ci mais entraîne la défaillance de tout ou partie de la société, en mobilisant de façon instantanée des chaines d'effets imbriqués. Par ce biais, la cybersécurité vient se rapprocher télologiquement d'une menace à caractère environnementale dont l'enjeu est le destin de la planète. Pour Lene Hansen et Helen Nissenbaum, la combinaison de catastrophes en cascade et de l'absence d'incident préalable de cette ampleur entraîne une situation paradoxale dans le discours sur la cybersécurité. D'un côté, l'hypersécuritisation et les discours qui la portent peuvent apparaître comme exagérés ; de l'autre côté, l'ampleur de la catastrophe annoncée peuvent donner à ces discours une valeur d'avertissement qu'il devient difficile d'ignorer. Du point de vue de cette recherche, ce phénomène participe ainsi à renforcer

⁸²⁶ Concept introduit dans les études de sécurité par l'ouvrage BUZAN Barry, *The United States and the Great Powers: World Politics in the Twenty-First Century*, Cambridge, Polity, 2004, 240 p.

⁸²⁷ Cf. nos éléments sur les discours catastrophistes.

l'aura terrifiante des menaces liées à la sécurité de l'information et ne facilite pas la discussion et la prise de recul sur l'objet-référent de ces discours.

Afin d'améliorer la crédibilité de l'hypersécurisation et de valider la conformité de l'individu dans la protection de la sécurité des réseaux d'appartenance de celui-ci, le discours sur la cybersécurité vient mobiliser les expériences individuelles. Cette mobilisation se traduit par une pratique quotidienne de la sécurité à l'échelle individuelle et organisationnelle. Le principal atout de ces pratiques quotidiennes est qu'elles traduisent la menace abstraite en expériences concrètes. Ce n'est pas tant la sécurité individuelle qui est l'objectif que l'appartenance de l'individu au public (*audience*) d'un discours de sécurité plus large. Il s'agit ici de créer un lien entre le public visé par le discours et la menace par le biais de l'identification⁸²⁸. La sécurisation de la vie quotidienne mise en lien avec l'hypersécurisation implique l'oblitération de la vie quotidienne des individus par les usages malveillants des réseaux. Dans ce cadre, l'institution de l'individu, non seulement en tant que partenaire responsable de la lutte contre la sécurité, mais également en tant que vecteur ou source de menace apparaît comme spécifique à la cybersécurité en tant que secteur. C'est ici que la confrontation entre postures technophiles et technophobes trouve son plus grand paradoxe. L'acteur instaure une responsabilité morale individuelle qui peut facilement faire passer le sujet, impuissant à insouciant, voire dangereux. Toutefois, l'acteur qu'il soit une entreprise ou un État ne souhaite pas que son public se passe des technologies de l'information. C'est ici la marque de ce qui apparaît dans cette recherche comme la dépendance à l'information et qui constitue la limite et donc la mesure de la cybermenace.

La technification apparaît comme le dernier phénomène lié à la cybersécurité en tant que secteur. Elle apparaît comme une fétichisation de l'expertise du technicien, qu'il soit informaticien ou hacker. Par son expertise, l'informaticien et le hacker ont accès à une forme de nouveau savoir mystique qui est constituée par la technique informatiques. C'est une étape essentielle de la sécurisation qui implique une forme de professionnalisation de la sécurité du

⁸²⁸ L'identification d'un acteur avec les sentiments, les besoins et les intérêts du public apparaît comme nécessaire au succès de la sécurisation. BALZACQ Thierry op-cit, 2016 p. 194.

fait de la grande importance qui lui est accordée. Lene Hansen et Helen Nissenbaum décrivent la technification comme la création d'un espace particulier pour le discours technique.

« Le rythme époustouflant auquel les nouvelles technologies et, à partir de là, les méthodes d'attaque sont introduites ajoute à la légitimité accordée aux experts et à l'autorité épistémique dont disposent les informaticiens qui leur confèrent le rôle privilégié de ceux qui ont le pouvoir de parler de l'inconnu. »⁸²⁹

Au-delà du caractère utopique que cela implique concernant les nouvelles technologies, la constitution d'une autorité experte dans les technifications implique une mise en relation ténue mais existante entre la connaissance légitime et la connaissance perçue comme illégitime. Autrement dit, la technification établit un lien entre l'informaticien et le hacker. Les auteures affirment que cette domination de la pensée technique vient cacher les racines politiques du phénomène et constitue également une source de légitimité nouvelle pour l'hypersécurisation. Au sujet de la technique, nos analyses sur le rapport entre cyberspace et technique ne peuvent également que souscrire à cette conclusion⁸³⁰.

Du point de vue de cette recherche, l'approche de Hansen et Nissenbaum attire l'attention sur la façon dont le discours a été défini principalement dans le contexte de la sécurité étatique. Leur typologie des grammaires du secteur de la cybersécurité met en lumière les nombreux mécanismes par lesquels cela s'est produit. Cependant, l'émetteur n'est que peu traité et le postulat de base entretient la forme confuse de la notion.

Le point positif de cette typologie est désormais que nous disposons apriori d'un début de grille qui vise à comprendre le lien théorique entre le langage cyber et la sécurisation. Nous disposons par cette grille d'un lien construit entre l'emploi d'un langage et l'objet de référence. Cette théorie repose principalement sur la mise en évidence de multiples discours à l'intérieur et au travers les frontières géographiques et politiques des États. Manifestant des contestations, ces discours sont considérés que constellations d'objets de référence connectés entre elles. De ce point de vue, par le biais des mécanismes identifiés les auteures suggèrent que la cybersécurité est centrée sur le lien que « le réseau » et « l'individu » entretiennent avec les

⁸²⁹ HANSEN Lene et NISSENBAUM Helen, 2009, op-cit, pp. 1166-1167. (Notre traduction)

⁸³⁰ Cf. chapitre 1

sécurités de la nation et de l'État⁸³¹. S'ils ne sont pas propres au secteur de la cybersécurité, les trois mécanismes (hypersecuritisation, pratique quotidienne et technification) sont suffisamment distinctifs au sein de la cybersécurité pour parler d'un secteur autonome.

En dépit des critiques que l'on peut soulever à l'égard de cette grille d'analyse, il faut souligner qu'elle a connu un important succès dans les travaux de recherche consacrés à la cybersécurité et plus largement à la question de la sécurité de l'information. La plupart des auteurs mobilisant ces grilles l'ont étendue à d'autres États que l'Estonie. Sur le cas français, on peut mentionner l'utilisation de la grammaire de la cybersécurité dans un article de Saïd Haddad consacré à la cyberdéfense⁸³². D'autres auteurs utiliseront cette grille pour approfondir les postures relatives aux discours de sécurité, c'est notamment le cas des travaux sur la technification de Prince et Lacy⁸³³.

B – Une illusoire autonomie de la sécurité face aux limites du discours.

Du point de vue de cette approche de la cybersécurité, la distinction de celle-ci des autres secteurs de la sécurité s'établit à partir de l'interaction entre les trois « grammaires » du discours. Il semble y avoir là une confusion entre le secteur et l'objet. Au contraire, le fait que ses éléments soient présents dans d'autres discours de sécurité et puissent opérer un appareil cohérent hors des secteurs concernés vient contredire l'applicabilité du concept de secteur à la cybersécurité. L'idée selon laquelle l'objet est transversal à tous les secteurs ne suffit pas à créer un secteur particulier autonome du reste. D'autant plus que le « secteur » créé ne saurait être particulièrement autonome car il n'opère pas uniquement selon ses propres règles, mais se détermine principalement par les pratiques sociotechniques liées à l'implémentation de l'objet-référent dans le secteur concerné.

Il pourrait également être reproché à cette grille de considérer tous les enjeux liés à la sécurité de l'information comme un enjeu unique malgré la multiplicité des discours sans même avoir recours aux grandes divisions qui pourraient rejoindre l'idée des secteurs (cyberdéfense,

⁸³¹ DEIBERT, 2002, op-cit,

⁸³² HADDAD, Saïd. « Une grammaire de la cybersécurité française ou la construction d'une stratégie nationale de cyberdéfense (2008-2017) », *Stratégique*, vol. 117, no. 4, 2017, pp. 119-135.

⁸³³ LACY Mark et PRINCE Daniel, « Securitization and the Global Politics of Cybersecurity. », *Global Discourse*, vol. 8, no. 1, 2018, pp. 100–115

cybercriminalité, cybersécurité, cyberdiplomatie) et qui se traduisent différemment du point de vue des enjeux concernés. L'idée d'un énième secteur autonome vient alors contredire l'applicabilité de ce concept à la cybersécurité. Car plus grand est le degré d'autonomie de la cybersécurité, plus forte est en réalité la ressemblance entre les secteurs où elle s'implémente du fait de sa transversalité. Autrement dit, du point de vue de la sécurité de l'information, il n'y a pas ou plus de secteurs. Demeure alors une question, s'il n'est pas ontologiquement pertinent d'avoir recours à l'autonomie, cette notion sert-elle un intérêt épistémologique ? L'idée d'autonomie traduit la spécificité des grammaires du discours et permet de faire le lien entre une vision classique de la sécurisation et l'objet d'analyse⁸³⁴. Dans ce contexte, l'idée de secteur intervient principalement comme une grille analytique et fonctionnelle plutôt que comme un outil descriptif. Or par sa complexité et sa pluralité, le discours dépasse ici les limites traditionnelles de ces secteurs.

Deux dimensions sont susceptibles de venir enrichir cette grille de lecture : le caractère approximatif du langage employé lorsqu'il s'agit de sécurité de l'information et le caractère controversé du langage étudié.

1 – L'approximation du langage : l'exemple de la critique du cyberterrorisme de Conway.

Au-delà de la méfiance nécessaire à l'égard des éléments techniques des définitions employant le label « cyber », il importe également de se méfier de leur contenu politique qui fait souvent l'objet d'exagération et dont les contours sont flous y compris dans la littérature académique⁸³⁵. Dans une étude de 2002⁸³⁶, Maura Conway interroge le concept le concept de cyberterrorisme à l'aune des pratiques numériques des organisations terroristes.

⁸³⁴ En effet, selon l'Ecole de Copenhague, le concept de secteur forme le cadre de la sécurisation (où l'on parle de sécurité). BUZAN Barry, WÆVER Ole et WILDE (DE) Jaap, 1998, op-cit.

⁸³⁵ Si ce flou implique la méfiance, il ne doit pas pour autant être vu comme une faiblesse ou une incapacité de l'acteur à décrire la menace. Voir KRIEG-PLANQUE Alice, *Analyser les discours institutionnels*, Paris, Armand Colin, 2012, pp. 155-185.

⁸³⁶ CONWAY Maura, « What Is Cyberterrorism? » *Current History*, vol. 101, n°659, Decembre 2002, pp. 436-442.

En tant que notion, le cyberterrorisme appelle deux clarifications pour pouvoir être employé. La première concerne la confusion entre le cyberterrorisme et la cybercriminalité. En partie à l'absence de définitions claires des deux phénomènes, cette confusion impacte le périmètre du cyberterrorisme en l'élargissant à des faits qui ne sont normalement pas du terrorisme classique⁸³⁷. La seconde précision consiste normalement à établir des distinctions claires entre l'utilisation terroriste des ordinateurs pour faciliter les activités de l'organisation et le terrorisme faisant appel à la technologie informatique de façon belliqueuse comme une arme ou comme une cible. Afin de résoudre ces deux difficultés, l'auteure considère que la cybercriminalité et le cyberterrorisme ne sont pas « coïncidents » (*coterminous*). Les attaques dans le cyberspace doivent comporter un élément « terroriste » pour être qualifiées de « cyberterrorisme ».

L'auteure assimile l'acte terroriste à un acte ayant des motivations politiques et entraînant la terreur du fait de morts et de destructions « à grande échelle ». Dès lors, le cyberterrorisme doit remplir ces critères pour être désigné comme tel⁸³⁸. Le cyberterrorisme vient s'insérer dans une typologie des pratiques politiques de l'information par des acteurs non-étatiques : usage (moyen de communication), mésusage (compromettre un site Internet ou un service), usage offensif (du fait de la présence de dégâts matériels ou d'un vol de données) et enfin viendrait le cyberterrorisme tel que décrit précédemment. Cette typologie implique que la grande majorité des activités terroristes sur Internet se limite à un usage et n'entre que rarement dans la catégorie du cyberterrorisme malgré les représentations qui en sont véhiculées.

L'article va également dans ce sens en affirmant que l'essentiel des preuves montre que les groupes terroristes utilisent largement Internet, mais qu'ils n'ont jusqu'à présent pas eu recours au cyberterrorisme ni montré leur volonté de s'engager lourdement dans cette direction. À l'image des cyberarmes, cela disqualifie une grande partie des utilisations du terme cyberterrorisme. Cette critique soulève ainsi des problèmes ontologiques plus vastes dans la littérature sur la cybersécurité. L'ambiguïté des termes dans la littérature peut s'étendre à l'attaque, à la sécurité, à la guerre, au crime dont l'emploi dénote une forme d'exagération...

⁸³⁷ Cela renvoie à des travaux postérieurs de l'auteure notamment sur la définition de la menace et l'impact du 11 septembre 2001 que nous évoquions en chapitre 3. CONWAY, 2009, op-cit.

⁸³⁸ L'auteure se réfère aux travaux de Dorothy Denning. Voir par exemple DENNING Dorothy E., « Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy », *Global Problem Solving Information Technology and Tools*, Décembre 1999, 30 p.

Toutefois au-delà de l'exagération, cette critique montre qu'il est dur de se représenter le phénomène en faisant fi de tout rapport à l'acteur.

2 – Controverses du langage et sécurité de l'information.

Un deuxième obstacle à la constitution d'une cybersécurité « autonome » tient compte d'un autre problème ontologique lié au langage « cyber ». Le langage est différent de la sécurité. En effet, sauf théorie contraire, la cybersécurité n'est pas l'objet référent de la sécurisation. Ce phénomène du langage est par ailleurs en concurrence avec d'autres notions et concepts s'inscrivant eux-aussi dans le processus de sécurisation de l'information (sphère informationnelle, renseignement, intelligence économique, etc.). Quand bien même l'enjeu de la sécurité de l'information est bien diffusé dans le monde, cette diffusion n'est pas nécessairement le fait du langage cyber.

Par ailleurs, la sécurité de l'information n'est pas forcément et intégralement comprise dans le cyberspace et ses termes dérivés. Ces derniers ne sont limités qu'à certains enjeux et montrent rapidement leurs limites quand il s'agit d'englober la totalité des aspects de la sécurité de l'information. Il est théoriquement possible d'accroître sans fin la liste des cybtermots, mais les cybtermots n'ont pas tous le même succès. En témoignent dans la littérature et les événements scientifiques, le déclin de l'emploi des notions de cyberguerre, de cybercontrefaçon, ou encore (justement) de cyberspace... Ou encore, l'absence presque totale de terme spécifique pour venir décrire l'enjeux de la manipulation de l'information quand bien même il était possible d'imaginer la cyberinfluence, ou la cyberpropagande⁸³⁹. Le langage « cyber » n'est qu'un artefact parmi d'autres. Leur emploi sert à opérer la transformation de l'information en enjeu de sécurité. Ce n'est par ce qu'il existe un discours de sécurité lié à un enjeu que ce discours devient lui-même l'enjeu.

Il faut prendre soin d'éviter la confusion entre le phénomène du langage et l'objet. Puisque le phénomène linguistique du cyberspace est un discours consacré à la sécurité de

⁸³⁹ Voir notamment JEANGENE-VILMER Jean-Baptiste, ESCORIA Alexandre, GUILLAUME Marine et HERRERA Janaina. *Les Manipulations de l'Information, un défi pour nos démocraties*, rapport conjoint du Centre d'analyse, de prévision et de stratégie (CAPS, ministère de l'Europe et des Affaires étrangères) et de l'Institut de recherche stratégique de l'École militaire (IRSEM, ministère des Armées), Paris, aout 2018, 214 p.

l'information. Ce n'est pas le seul discours qui existe sur ce sujet. Ce n'est pas forcément non plus le « meilleur » discours.

Enfin, si nous associons la différence entre sécurité et langage à l'approximation de ce dernier, nous définissons un espace de controverse qui fait la part belle à une définition subjective du langage et donc aux phénomènes d'influence et de résistance dans la sécurisation de l'information. Le langage en général, et les termes dérivés du cyberspace en particulier, tiennent un rôle prépondérant dans ce processus. Dès lors, le processus de sécurisation identifié ne peut apparaître comme autonome du fait de cette nécessaire controverse. C'est tout l'apport du concept de communauté épistémique à la compréhension du phénomène discursif⁸⁴⁰. Cette communauté particulière désigne ici le phénomène dynamique de redistribution des rapports de force dans l'espace sémantique relatif à un enjeu (la sécurité de l'information).

Cela traduit ici la profonde dépendance de la sécurisation de l'information à l'environnement dans lequel évolue l'acteur sécurisant. La sécurité de l'information n'est pas une nouvelle forme de sécurité, mais une « nouvelle variable » qui vient questionner les définitions antérieures de la sécurité. Encore une fois, l'idée de secteur semble ici inapplicable. Cette absence d'utilité devient préjudiciable lorsque le phénomène discursif fait déjà l'objet de nombreuses fractures qui viennent limiter la possibilité de lier les différentes espèces à un phénomène commun. Fractures que cette grille d'analyse élude au profit d'une seule grille analytique indépendante de l'acteur.

Les études de sécurité semblent ainsi pouvoir opérer une traduction du phénomène du langage en phénomène susceptible d'être vu du point de vue des Relations Internationales grâce au concept de sécurisation et peuvent en isoler quelques manifestations matérialisées par les « grammaires ». Toutefois les considérations liées à l'autonomie et aux secteurs ne nous semblent pas utiles à la compréhension du phénomène. Pour rappeler les mots de notre chapitre liminaire, la sécurisation devient « l'opérateur de conversion » validant l'affrontement des rhétoriques politiques au sein du champ politique qui valorise ou dévalorise certaines menaces. Cet opérateur acquiert force de vérité par les professionnels de la gestion de la menace, en

⁸⁴⁰ Cf. chapitre 3. Les éléments récoltés au cours de cette recherche sont parvenus à mettre en lumière une certaine influence américaine sur la définition de la forme et du contenu du discours analysé. Sur l'importance des professionnels et de la légitimité pour la labellisation, BIGO 1998, op-cit. p. 70-71

fonction des transformations de la violence qu'ils observent et de leurs intérêts en tant qu'institutions. Ce sont ces institutions de sécurité qui créent leur objet comme objet légitime de discours en y investissant des hommes, du temps de travail, des appareils statistiques, des routines qui donnent corps aux labellisations politiques. Cette théorie explique ainsi comment la cybersécurité se construit et influence le politique. Toutefois, il n'y a pas d'explication des raisons pour lesquelles cette transformation de l'information s'opère. C'est toute la limite de la théorie de la sécurisation.

C – Recontextualisation de la sécurisation de l'information.

Afin d'envisager ce pourquoi l'information devient un objet de sécurité, il faut mobiliser d'autres approches que celles de la sécurisation. Ces approches doivent permettre de remettre en contexte la sécurité de l'information. La question n'est plus de savoir comment le cyberespace et les termes dérivés agissent en tant que discours de sécurité, mais de comprendre si cette action appartient à un phénomène plus vaste. Il ne s'agit pas tout à fait d'inclure les pratiques non-discursives que nous avons pu identifier par ailleurs mais de prendre un peu de recul sur le phénomène.

Cette prise de recul peut s'envisager de trois manières. Tout d'abord, il peut être utile de résister au label « cyber » dans l'évolution des labels depuis la fin de la deuxième guerre mondiale. Nous nous intéresserons en particulier aux labels destinés à qualifier les formes de conflits. Ce n'est pas le seul exemple, mais cela permettra d'examiner les différents usages de l'information dans ceux-ci et d'établir un rapport entre technologie et conflit. La deuxième solution pour prendre du recul sur le langage consiste à dépasser l'idée d'autonomie en associant la sécurité de l'information avec d'autres enjeux fonctionnant dans une logique semblable. Nous exploiterons en particulier la convergence entre les enjeux de sécurité de l'information et le terrorisme. Enfin, dans une troisième étape, nous pousserons plus loin notre raisonnement en ayant recours à l'idée de transformation de la sécurité par l'intervention des acteurs non-étatiques.

1 – Le « cyber- », un label comme les autres ? Les conflits postmodernes de Gray.

Dans le deuxième chapitre de son ouvrage *Peace, War, and Computers*⁸⁴¹, Chris Hables Gray cherche à comprendre la transformation de la guerre depuis la fin de la Seconde Guerre mondiale. La survenance d'une arme absolue combinée à la continuité de la bataille et à la globalization des conflits, ont entraîné l'évolution de la guerre d'une conception encore moderne du politique à une conception postmoderne de celui-ci. Assimilé à la guerre des États-nations, la guerre moderne pour l'essentiel demeure en place (complexe militaro-industriel, la technologie⁸⁴², et l'association entre la guerre et l'idée de moyen efficace). La transition entre les deux systems est liée pour l'auteur à la remise sur le devant de la scène de la “guerre de guerillas et de ses cousins” (L'auteur comprend dans cette expression à la fois les petites guerres, les guerres sales, les guerres limitées ainsi que les conflits ethniques). Un autre élément de cette transition est la mutation de la mobilisation scientifique en révolution permanente des affaires militaires et la production devenue constante de nouvelles armes automatisées et électroniques. En résumé, la guerre postmoderne mobilise ainsi selon l'auteur des reprises de la guerre moderne, les nouvelles technologies et des acteurs non-étatiques.

Il y aurait sans doute beaucoup à dire sur le postulat de départ, l'ontologie du concept de guerre proposée et l'emploi de la postmodernité pour parler de la guerre et l'influence de la « *French Theory* »⁸⁴³. De manière générale, les postmodernes qui étudient la guerre insistent sur les informations, le langage et l'utilisation de symboles, traditions, mythes, techniques, effets et métaphores comme base pour construire des vérités. Cette insistance contribue à

⁸⁴¹ GRAY Chris Hables (2005). *Peace, War and Computers*. Londres, Routledge, 2013, 240 p.

⁸⁴² L'auteur mobilise à la fois technologie et « technoscience » dans l'ouvrage de façon un peu confuse. L'auteur ayant travaillé sur le concept de cyborg, nous pensons qu'il proviendrait de la lecture de Donna Haraway, elle-même reprenant l'acception de Bruno Latour. Le terme est popularisé par Gilbert Hottois en 1978. HOTTOIS Gilbert, « Ethique et techno-science », *La pensée et les hommes*, n° 22, 1978 pp. 111 – 116. Pour une étude voir HOTTOIS Gilbert. « Chapitre 22. Philosophie de la technique et des technosciences », In. HOTTOIS Gilbert (dir), *De la Renaissance à la Postmodernité. Une histoire de la philosophie moderne et contemporaine*, De Boeck Supérieur, 2005, pp. 485-532. Pour une histoire de la création du concept et l'évolution de son sens voir HOTTOIS Gilbert. « La technoscience : de l'origine du mot à ses usages actuels », *Recherche en soins infirmiers*, vol. 86, no. 3, 2006, pp. 24-32. LYOTARD Jean-François. *Le Postmoderne expliqué Aux Enfants: Correspondance, 1982-1985*. Galilée, 1986, 165 p. LATOUR Bruno *Science in Action: How to Follow Scientists and Engineers through Society*, Harvard University Press, 1987, 274 p. HARAWAY Donna J. *Modest Witness Second Millennium: Femaleman Meets Oncomouse: Feminism and Technoscience*. Routledge, 1997, 361 p.

⁸⁴³ Voir notamment à ce sujet CUSSET François (2003), *French Theory. Foucault, Derrida, Deleuze & Cie et les mutations de la vie intellectuelle aux États-Unis*. Paris, Éditions La Découverte, 2005, 352 p.

redéfinir une nouvelle forme de la guerre. La guerre postmoderne rejette la croyance moderne en l'existence de principes immuables qui s'appliqueraient à la guerre. Cette guerre postmoderne aurait pour particularité de brouiller les frontières entre civil et militaire, de placer l'information au cœur de son dispositif à la fois dans la conduite de la guerre mais également dans la saturation des médias.

Parmi les signes de l'émergence de la guerre postmoderne, Chris Gray pointe en particulier la multiplication des labels pour qualifier la guerre depuis la fin de la deuxième guerre mondiale⁸⁴⁴. Les premiers éléments de cette typologie concernent les années 45 à 50 qui voit émerger tour à tour les notions de guerre atomique (*atomic war*), guerre nucléaire (*nuclear war*) et guerre thermonucléaire (*thermonuclear war*) en parallèle de la consolidation du concept de guerre de froide. L'auteur ne mentionne pas la théorisation de la guerre perpétuelle en 1953⁸⁴⁵.

Au contraire, la typologie opère un saut jusqu'au début des années 70. Quatre concepts apparaissent alors : La guerre technologique (*technology war / technological warfare*) attribuée à Possony et Pournelle⁸⁴⁶, qui est l'application directe et délibérée de la base technologique nationale et des avancées spécifiques générées par cette base pour atteindre des objectifs politiques, stratégiques et tactiques⁸⁴⁷. Le deuxième label est le militarisme USA (*militarism USA*) de l'ancien colonel du corps des marines James A. Donovan qui apparaît comme une critique du poids de du budget et des politiques militaires des États-Unis mis en parallèle de son inefficacité au Vietnam.⁸⁴⁸. Un peu plus tard dans les années 70, émergeront les concepts

⁸⁴⁴ GRAY Chris Hables, op-cit, pp 23-24.

⁸⁴⁵ BARNES Harry Elmer (dir). *Perpetual War for Perpetual Peace: a Critical Examination of the Foreign Policy of Franklin Delano Roosevelt and Its Aftermath*. Caldwell, Caxton Printers, 1953, .

⁸⁴⁶ Gray place la naissance de la *technological warfare* en 1986, mais elle est déjà présente dans l'ouvrage en question : POSSONY Stefan Thomas et POURNELLE Jerry, *The Strategy of Technology; Winning the Decisive War*. University Press of Cambridge, 1970, 189 p.

⁸⁴⁷ Ibid, Chapitre 1, p. 4.

⁸⁴⁸ DONOVAN James, A., *Militarism, U.S.A.* New York, Scribner, 1970, 265 p.

de guerre sans fin (*war without end*)⁸⁴⁹ et de guerre permanente (*permanent war*)⁸⁵⁰. Une autre absente de cette typologie est la guerre cybernétique proposée en 1979 par Jonathan Vos Post⁸⁵¹.

Au début des années 80, de nombreux labels émergent alors que la *Cool War* naît sous la plume de l'auteur de science-fiction Frederik Pohl⁸⁵² et décrit une guerre dans laquelle chaque État tente de saboter les économies de ses rivaux, même s'ils sont politiquement alliés. L'*AirLand Battle* se popularise dans l'armée américaine et *Star Wars* quitte le domaine de la science-fiction pour devenir synonyme au début des années 80 du programme de défense antimissile *Strategic Defense Initiative* destiné à la protection des États-Unis contre une frappe nucléaire stratégique. Les années 80 seront particulièrement riche au niveau des labels proposés.

En 1983, Sylvère Lotringer et Paul Virilio ont développé à travers une série d'entretiens une nouvelle lecture du concept de guerre pure (*Pure War*)⁸⁵³. Dans cette conception, la guerre et sa logistique nécessitent une rapidité et une efficacité accrues, et la technologie fournit des instruments qui créent des instruments de guerre de plus en plus meurtriers et efficaces. L'accélération de la vitesse et de la technologie crée à son tour une industrie plus dynamique et un système industriel qui efface les différences de temps et d'espace grâce au développement des technologies de transport, de communication et d'information. L'ensemble des réalisations humaines sont le produit de la mobilisation et du déploiement militaires. La guerre est donc le moteur de l'histoire. Elle crée le développement technologique tout autant qu'elle représente l'une des ultimes menaces envers l'humanité dans la menace d'un holocauste nucléaire.

La première moitié des années 80 est marquée par deux autres labels. Le premier est les guerres mentales (*Mind Wars*) qui traite du potentiel militaire des armes psychiques⁸⁵⁴. Le

⁸⁴⁹ KLARE Michael T., *War Without End: American Planning for the Next Vietnam*, New York, Knopf, décembre 1972, 464 p.

⁸⁵⁰ MELMAN, Seymour. *The Permanent War Economy; American Capitalism in Decline*. New York, Simon and Schuster, 1974, 384 p.

⁸⁵¹ VOS POST Jonathan, 1979, op-cit.

⁸⁵² POHL Frederick Julius. *The Cool War*. Corgi, 1983, 288 p.

⁸⁵³ VIRILIO Paul et LOTRINGE, Sylvère, *Pure war*. New York, Semiotext(e), 1983, 174 p. Voir également des mêmes auteurs VIRILIO Paul et LOTRINGER Sylvère *Pure war : twenty-five years later*, Los Angeles, MIT Press, 2008, 253 p.

⁸⁵⁴ MCRAE, Ronald M. *Mind Wars: the True Story of Government Research into the Military Potential of Psychic Weapons*. New York, St. Martins Press, 1984, 155 p.

second nous intéressera davantage puisqu'il s'agit de l'application du postmodernisme à l'idée de guerre (*postmodern war*) réalisée aussi en 1984 par Frédéric Jameson en grande partie à propos de la guerre du Vietnam⁸⁵⁵. Ce conflit est décrit comme une des premières guerres postmodernes. Laquelle modifie les représentations et ne peut plus être culturellement représentée de manière traditionnelle du fait du bon technologique qui a été le sien. Durant la seconde moitié et la fin des années 80, l'émergence des labels croît. Une dizaine de nouveaux concepts va voir le jour. Parmi ces concepts, une grande partie est directement liée à la technologie et à son utilisation : la guerre de haute-technologie (*high technological war*)⁸⁵⁶, technoguerre (*technowar*) et la guerre parfaite (*perfect war*)⁸⁵⁷, la guerre informatique (*computer war*)⁸⁵⁸ et bien sur la cyberguerre (*cyberwar*)⁸⁵⁹. Chris Gray ne le mentionne pas mais la fin des années 80 sera également l'occasion de voir réémerger le *war-gaming* en particulier à l'US Naval War College⁸⁶⁰. Dans la lignée de ces concepts seront également développés à l'époque les concepts de conflit de basse intensité qui rentre dans la doctrine de l'armée américaine à partir de 1986 ainsi que d'*Imaginary War*⁸⁶¹ et de *Time Wars*⁸⁶².

Les années 90 forment le début de la littérature sur le champ de la guerre de l'information et de « l'infoguerre ». En dehors de la guerre de l'information, c'est environ 24

⁸⁵⁵ JAMESON Fredric, (1984) *Postmodernism, or the Cultural Logic of Capitalism*. Durham, Duke University Press, 1984, 438 p. Voir également GRAY Chris Hables. *Postmodern War: the New Politics of Conflict*. New York, Guilford Press, 1997, 314 p.

⁸⁵⁶ EDWARDS Paul Norris, *Artificial intelligence and high technology war: the perspective of the formal machine* Silicon Valley Research Group, University of California, Santa Cruz, 1986, 90 p. Voir également de cet auteur en 1986 : « Border Wars: The Science and Politics of Artificial Intelligence », *Radical America* vol. 19, no. 6, 1986, pp 39-50.

⁸⁵⁷ GIBSON James William. *The Perfect War: Technowar in Vietnam*. Boston, Atlantic Monthly Press, 1986, 523 p.

⁸⁵⁸ VAN CREVELD Martin, *Technology and War: From 2000 B.C. to the Present*, Washington, D.C, Free Press, 1989, 342 p.

⁸⁵⁹ Invention du terme : DAVIES Owen, 1987, op-cit. ; Premières utilisations : DERIAN James, *Cyberwar, Video Games, and the New World Order*, Second Annual Cyberspace Conference, Santa Cruz, Avril 1991 ainsi que ARQUILLA John et RONFELDT David, 1993 op-cit.

⁸⁶⁰ MASTERSON, Rear et al. « New Concepts in Global War-gaming », *Proceedings—US Naval Institute*, juillet 1987, pp. 117-119.

⁸⁶¹ KALDOR Mary « The Imaginary War » In. SMITH Dan, et THOMPSON Edward Palmer (dir.). *Prospectus for a Habitable Planet*. Penguin, 1987. Pour une étude plus avancée du concept, voir KALDOR, Mary. *The Imaginary War : Understanding the East-West Conflict*. Cambridge, Basil Blackwell, 1990, 298 p.

⁸⁶² RIFKIN Jeremy, *Time Wars: The Primary Conflict in Human History*, New York, Simon & Schuster, juin 1987. 302 p.

labels différents qui ont émergé. Ce n'est pas la finalité du présent travail de recherche d'en mentionner l'intégralité mais certains sont très proche de l'idée de guerre de l'information : par exemple on retrouve en 1991, l'*High Modern War*⁸⁶³ et l'*Hyper Modern War*⁸⁶⁴ ou en 1993, la *Netwar*⁸⁶⁵, la *Third Wave War*⁸⁶⁶. Parmi les notions plus avancées, les guerres de *command and control* (C2) ou les guerres réseau-centrée (*Network centric warfare*)⁸⁶⁷ concernent également l'information de manière directe. Les années 2000 verront également les labels exploser avec une dizaine de nouveaux items dès les premières années. Nous retiendrons tout particulièrement le concept d'*Internet War* formulé en 2001 par Thomas Keenan⁸⁶⁸.

Les labels de la guerre semblent avoir plusieurs caractéristiques intéressantes. D'un point de vue thématique, ils n'échappent pas à une certaine forme de redondance descriptive dans les phénomènes qu'ils cherchent à englober. L'information et la technologie sont une tendance forte au sein de ces néologismes qui s'accroît avec le temps. Sur la forme, la croissance du nombre de label se poursuit et augmente au fur à mesure des années. Entre les années 70 et le début des années 2000, le rythme d'émergence semble avoir triplé. Cependant, il est assez difficile de dépasser cette labellisation car toutes les théories de la guerre centrée sur l'information, qu'il s'agisse de guerre en réseau, de guerre virtuelle, de cyberguerre apparaissent comme appauvries et du domaine du « vœu pieux »⁸⁶⁹. Le vrai rôle de l'information dans la guerre postmoderne apparaît comme plus compliqué que la simple tentative de labellisation dont elle fait l'objet. La technologie n'est qu'un petit élément de celle-ci. En effet du point de vue de la guerre, le progrès technique compte moins que le fait de disposer de la technologie appropriée. Chris Gray attribue cette prolifération de nouvelles théories de guerre à deux crises interdépendantes. Premièrement, la transformation induite par le pouvoir croissant des

⁸⁶³ DER DERIAN., 1991, op-cit.

⁸⁶⁴ Attribué à Donna Haraway.

⁸⁶⁵ ARQUILLA John et RONFELDT David, 1993 op-cit.

⁸⁶⁶ TOFFLER Alvin, et TOFFLER Heidi. *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston, Little, Brown & Co, 1993, 302 p.

⁸⁶⁷ CEBROWSKI, Arthur K. et GARSTKA John J., « Network-Centric Warfare: Its Origins and Future, » U.S. Naval Institute Proceedings, Annapolis, Maryland, Janvier 1998.

⁸⁶⁸ KEENAN Thomas, « Looking like Flames and Falling like Stars: Kosovo, “the First Internet War” », *Social Identities*, vol. 7, no. 4, 2001, pp. 539–550

⁸⁶⁹ GRAY, 2013, op-cit, p. 37.

technologies de l'information dans la culture contemporaine. Deuxièmement, il y a la crise de la guerre elle-même, qui est réduite à l'absurde avec la guerre postmoderne...

Rapportée au cyberespace en tant que discours de sécurité, une telle approche confine le phénomène à un emballage autour de l'enjeu de l'information. Cela permet de prendre du recul sur l'hypersécurisation qui semble animer ce discours de sécurité pour en faire un phénomène plus vaste qu'il n'est ainsi possible de faire remonter jusqu'au début des années 70. Cette période correspond à la deuxième vague de l'introduction de l'outil informatique dans les administrations publiques et représente la transition de la mécanographie à l'informatique⁸⁷⁰. En revanche la distinction entre information, technologie et connaissance demeure assez floue.

2 – La sécurité à l'âge digital chez Der Derian.

En décembre 2003, la revue *Millennium*, a publié un numéro spécial afin d'explorer l'impact des technologies de l'information sur les Relations Internationales⁸⁷¹. Ce numéro consiste en la publication des actes de la conférence annuelle de la revue s'étant déroulé au mois d'octobre de la même année. Il s'agissait à l'époque d'examiner les défis en matière de gouvernance que la révolution induite par les technologies de l'information pouvait entraîner. Trois types d'enjeux sont pointés du doigt à l'époque : le contournement des canaux de participation classiques pour l'influence de la décision politique par de nouveaux acteurs, la crise potentielle en matière de responsabilité démocratique, de légitimité et d'identité, et enfin la conception changeante de la manière dont les États définissent leurs intérêts (sécurité, contrôle, puissance). C'est surtout le dernier point qui va nous intéresser à ce stade du développement. Cependant, ce numéro spécial constitue une base de réflexion sur les technologies de l'information qui alimente non seulement le débat autour de la sécurité mais également d'autres thématiques comme celle du développement, de la gouvernance ou de la société civile dans les Relations Internationales. Parmi les auteurs de ce numéro spécial ayant travaillé sur la sécurité, nous avons déjà mentionné Ronald Deibert. Deux autres auteurs

⁸⁷⁰ Voir rapport post-doctoral précité, BAUDOT Pierre-Yves, juin 2007, op-cit.

⁸⁷¹ *Millennium: Journal of International Studies*, Vol.32, No.3, décembre 2003.

peuvent nous intéresser à ce stade pour recontextualiser la sécurisation de l'information : James Der Derian et Michael Dartnell.

Dans son article⁸⁷², James Der Derian se pose la question de savoir comment le numérique qui qualifie de *Digital Age* en est venue à profiter d'une forme d'hégémonie sur d'autres descripteurs de la modernité. Ontologiquement, il affecte ce *Digital Age* de propriété propre à une forme de singularité politique. En effet, à ses yeux, la caractéristique distinctive de cette ère nouvelle est : « une intensité spatio-temporelle plutôt qu'une extensivité géopolitique ; c'est-à-dire une capacité à intensifier les effets globaux à travers un effondrement du temps et de la distance »⁸⁷³. Il qualifie cette transformation d'« éternel retour nietzschéen » dans la mesure où la seule constante du phénomène se traduit par un changement rapide, récurrent et reproductible. En cela l'âge digital. Pour Der Derian, cela oppose l'âge digital et la révolution de l'information à une révolution politique ordinaire. La modernité numérique n'est pas synonyme d'un avant et d'un après. Elle se traduit par des oscillations rapides entre médium et message, des images mobilisées en boucle de rétroaction (*feedback*) et enfin des déphasages entre ordre et désordre qui induisent une forme de complexité. C'est véritablement un phénomène de singularité qui ressemble pour partie à ce que nous avons déjà identifié lors de notre analyse du cyberespace en tant que métaphore spatiale.

Néanmoins, n'étant pas contraint par un objet d'analyse particulier⁸⁷⁴, Der Derian porte cette réflexion à l'ensemble des technologies de l'information de la fin des années 40 jusqu'au 11 septembre 2001. A partir de cette ontologie, l'article adopte un questionnement en trois étapes.

D'une part, l'interrogation porte sur la discrimination de la nouveauté du phénomène et sur ce qui est le « plus transformateur »⁸⁷⁵ au sein de celui-ci. L'article opte pour une définition des technologies de l'information comme le produit de l'interaction du pouvoir, du savoir et de la technique, dans laquelle des archives sont créées, des connaissances codifiées, des

⁸⁷² DER DERIAN James. « The Question of Information Technology in International Relations. » *Millennium*, vol. 32, no. 3, décembre 2003, pp. 441–456,

⁸⁷³ Notre traduction. Ibid. p 442.

⁸⁷⁴ Le bornage temporel

⁸⁷⁵ Ibid. p. 444.

informations transmises, et les effets sont produits et commandé à distance⁸⁷⁶. Pour l'auteur, les technologies informatiques une fois mises en réseau fournissent aux nouveaux acteurs les moyens de traverser frontières politiques, économiques, religieuses et culturelles, ne changeant pas seulement la manière de faire la guerre et la paix, mais en flouant la distinction entre les deux.

D'autre part, l'article s'interroge sur les capacités accrues des technologies de l'information de servir de déclencheur et transmetteur des événements mondiaux ainsi sur les réponses diplomatiques et militaires qu'ils suscitent. Ici, Les nouveaux réseaux de pouvoir informationnels et technologiques internationaux requièrent de nouveaux modes de compréhension et d'enseignement. Les sciences sociales n'ont pas encore relevé le défi que cela représente au moment de la rédaction du texte. En effet, actualiser les événements mondiaux en temps réel à travers les frontières traditionnelles politiques, sociales et culturelles, les technologies de l'information résistent à la recherche qui tente de discerner des comportements rationnels, d'appliquer des modèles, ou de mener des projets de recherche incrémentiels. Par ailleurs, comme nous l'avons remarqué au cours de cette recherche, travailler sur ces objets implique à un dialogue avec de nombreux cercles non-académiques : industriels, militaires, administratifs. Ce travail s'oppose au modèle scientifique construit autour d'une discipline ou au modèle du think tank politiquement orienté.

« Nous avons besoin d'une stratégie qui approuve les approches conceptuelles, plurielles et multidisciplinaires pour étudier ce que nous considérons comme la question la plus difficile du XXIe siècle : l'application globale et le management des technologies de l'information temps de guerre et de paix. »⁸⁷⁷

Enfin, l'article propose une approche critique de la question connaissances existantes sur le fonctionnement de ces technologies vis-à-vis des Relations Internationales. Der Derian envisage deux modes de changement discursif particuliers pour l'idée de sécurité : la *mimesis* et la *poésie*. D'un côté, il existe une « poésie » dans laquelle une transformation positive de la pensée peut être provoquée pour construire de nouvelles formes possibles pour le discours sur la sécurité internationale. De l'autre côté, il y a « *mimesis* » où des images visuelles répétitives

⁸⁷⁶ Ibid. p. 450.

⁸⁷⁷ Ibid. p. 452.

et violentes (L'*infowar* ou infoguerre) peuvent conduire à un discours de sécurité beaucoup plus rigide. La guerre de l'information, ou infoguerre, est le concept pour comprendre la cyberguerre, les guerres de hackers, la *netwar*, guerre virtuelle et autres conflits réseaux-centrés. Du point de vue des exemples retenus cela inclus les opérations comme la propagande ou les opérations psychologiques. Et de nombreuses comparaisons sont effectuées avec les actions terroristes. Les deux processus de transformation se disputent une « bataille épistémique pour la réalité », autrement dit pour définir le discours sur la sécurité de l'information. Le discours sur la sécurité de l'information résulte ainsi d'un dialogue entre pessimise et optimisme sécuritaire. La cybersécurité semble incarner une forme « mimétique » de la sécurité de l'information. Elle n'insiste pas tant sur le fait que la technologie renforce la sécurité que sur la représentation d'un espace de menace. Si nous nous en référons à cette grilles interprétative le cyberespace et les termes dérivées ont une assiette réduite à moins de la moitié de la sécurité de l'information, ce qui diminue considérablement la portée du phénomène linguistique vis-à-vis de l'enjeu politique de l'information.

3 – L'identité et la transformation globale de la sécurité de Dartnell.

Dans un autre article du même numéro spécial⁸⁷⁸, Michael Dartnell s'interroge également sur la transformation de la sécurité, toutefois ce n'est pas tant la technologie qui l'intéresse sur un plan philosophique que les effets des pratiques technologiques dans la construction des perceptions et des identités⁸⁷⁹.

Pour Dartnell, la technologie de l'information incarne une transformation significative qui secoue les bases de la réalité. Il s'agit donc de démontrer comment l'outil informatique façonne les perceptions par l'introduction de valeurs, d'idées et d'identités qui transforment les notions de soi et de sûreté qui sont au cœur de la sécurité. Ici pour l'auteur, il est important de souligner qu'Internet n'est pas une menace pour les acteurs liés à la souveraineté au sens où cette technologie contournerait ou renverserait complètement les impératifs politiques et réglementaires du contrôle. Au lieu de cela, Michael Dartnell envisage avant tout la technologie

⁸⁷⁸ DARTNELL Michael. « Weapons of Mass Instruction : Web Activism and the Transformation of Global Security. » *Millennium*, vol. 32, no. 3, Dec. 2003, pp. 477–499,

⁸⁷⁹ Sur les identités et les technologies de l'information, HOLMES David, *Virtual Politics: Identity and Community in Cyberspace*, Londres, Thousand Oaks, 1997, 256 p.

comme un dispositif qui facilite les relations politiques. Néanmoins, la transformation induit une perte du contrôle de l'acteur régional sur la sécurité.

En effet, en se concentrant sur l'activisme comme objet d'étude, on s'aperçoit que le phénomène dépasse largement les limites classiques de l'acteur régional.

« La transformation est devenue familière grâce aux relais électroniques de la campagne pour l'interdiction des mines antipersonnel, du mouvement antimondialisation et, plus récemment, de la mobilisation de l'opinion publique mondiale contre l'intervention américaine en Irak. Dans ces exemples, les technologies de l'information transmettent les mouvements transnationaux aux contextes nationaux. En outre, les technologies de l'information permettent également aux groupes ciblés au niveau national de transmettre des points de vue locaux et nationaux sur la scène mondiale. »⁸⁸⁰

Cette combinaison de groupes nationaux et transnationaux implique une influence de l'identité qui dans tout contexte global pourrait provenir de n'importe quel autre environnement. Dans ce contexte, Dartnell vient distinguer trois espaces de pratiques qui relient les technologies de l'information à l'idée de sécurité globale : les pratiques militaires, la cybersécurité, et l'activisme sur Internet (*Web activism*)⁸⁸¹. Ce dernier se distingue de la cybersécurité pour l'auteur car il est avant tout centré sur les perceptions et redéfinit les limites de la sécurité globale. En effet, il y est possible pour des acteurs non-étatiques de fournir des informations qui rediffusent les formes et les contenus des identités. Les idées ne menacent directement ni les infrastructures critiques ni les capacités militaires, mais peuvent déstabiliser l'ordre politique et social en modifiant les notions des acteurs sur la sécurité, les menaces et la violence.

Dans cette étude, l'objet Internet est principalement présenté comme un assemblage de pratiques issus des anciens médias et d'une histoire qui remettent en cause l'aspect révolutionnaire de cette transformation de l'information. L'activisme montre à quel point les conflits contemporains se déroulent loin d'un champ de bataille, dans un large contexte médiatique formant un réseau global de communication et de conflit. Ce contexte accélère et intensifie la transgression, redéfinit et transforme les frontières de l'identité et de la politique

⁸⁸⁰ Ibid. p. 479. (Notre traduction)

⁸⁸¹ Pour approfondir cette notion d'activisme sur Internet, voir l'ouvrage collectif récent : MEIKLE Graham (dir.), *The Routledge Companion to Media and Activism*, New York, Routledge, mars 2018, 420 p.

en permettant de nouvelles réflexions, perceptions et expériences sociales résultant tout à la fois de globalisation et de l'invention de nouveaux modes de communication. Ainsi, en ce qu'elle permet à de nombreuses tendances politiques d'exister sur la scène mondiale, l'information met en place une nouvelle structuration du monde. C'est ce que Michael Dartnell décrit comme une scène globale « post-réaliste ». Il s'agit d'une sphère internationale dans laquelle la politique mondiale n'est plus une prérogative régaliennes, alors même que, paradoxalement, les États restent les acteurs les plus importants du pouvoir international.

« La transformation affectant le conflit, la sécurité et la centralité de l'État dans les affaires mondiales est liée de manière essentielle au monopole coercitif de la forme Westphalienne-Leviathan de l'État. »⁸⁸²

Or ici, la violence terroriste ou la violence déployée dans les nouvelles formes de conflit n'est plus déployée par des agents étatiques (bien qu'un soutien étatique soit toujours possible). En parallèle, les États ont pour la plupart peu de contrôle sur le contenu des technologies qui véhiculent des messages et transforment le champ des perceptions des acteurs. La technologie suggère que le pouvoir réel est relativement moins défini par son emplacement physique et que la contiguïté territoriale pourrait être moins en mesure d'influencer la forme des futures relations humaines, résultant en une forme d'hybridation du pouvoir. Pour l'auteur, la sécurité mondiale n'est pas renforcée si les défis sont relevés en termes « purement militaires », alors que les conflits sont « multiniveaux et de plus en plus innovants », construits « sur la représentation, la perception et l'image »⁸⁸³.

Section 3 – La réception des discours sur la sécurité de l'information dans les Relations Internationales.

La recontextualisation de la sécurité de l'information pour dépasser le phénomène du langage « cyber » entraîne un autre risque qui consiste à renvoyer la recherche vers une forme de déterminisme technologique. Nous quittons ainsi le domaine du discours « cyber » proprement dit pour nous confronter à un autre ensemble discursif : celui de la révolution de l'information. Nous avons déconstruit les rapports du cyberspace à la technique et à la fiction dans notre premier chapitre. Ici, il s'agit de plutôt d'extraire la sécurité de

⁸⁸² DARTNELL Michael, 2003, op-cit. p. 494 (Notre traduction).

⁸⁸³ Ibid. p. 499.

l’information en tant qu’objet de Relations Internationales par rapport à cette toile de fond. Si nous combinons les approches que nous venons d’évoquer.

La transformation de l’information en enjeu de sécurité opère avec et en dehors des discours tirés du cyberspace. Ils s’inscrivent dans un long processus lié à l’informatisation de la société et des États. Elle peut exister dans tous les endroits qui ont une pratique de l’informatique. Elle peut opérer selon deux modes : l’un positif, où les technologies renforcent la sécurité ; l’autre négatif, où elles sont vectrices de nouvelles menaces⁸⁸⁴. Ces approches optimistes et pessimistes qui font échos aux compréhensions philosophiques et sociologiques de la technique dont elles récupèrent une grande partie des développements. Cette transformation entraîne des effets politiques qui peuvent être étudiés. L’étude de ces effets rend possible l’étude de la transformation elle-même.

Afin de sortir de l’ambiguïté, il importe de reconnaître que sous couvert d’étudier la sécurité, la plupart des auteurs étudient en fait un phénomène qui implique trois objets différents reliés par la notion d’information : le langage, la sécurité et la technologie. Chacun de ces objets peut être décomposé en de nombreux artefacts de différente nature. C’est à partir de ce moment-là que la confusion peut opérer. C’est la raison de notre précaution en début de chapitre où ont été distinguées le phénomène du langage de l’objet référent, et des théories.

C’est toute la difficulté de l’étude. L’espace sémantique qui traduit le glissement de sens du langage « naturel » pour reprendre le terme de Passeron vers les théories (le monde logique) par le biais d’une similitude d’objet référent pourrait très bien illustrer ce phénomène de manière abstraite. Mais une fois que la transition du monde historique vers le monde logique s’est opérée, l’assiette du phénomène ne se limite plus à un seul phénomène du langage. Elle englobe toutes les théories qui peuvent servir la compréhension épistémologique de l’objet référent.

Malgré un succès des thématiques de l’information et de la cyberguerre en termes de publications, relativement peu d’articles et d’ouvrages ont été consacrés à la réception générale des technologies de l’information dans les Théories des Relations Internationales. La majorité

⁸⁸⁴ Comme toujours, il est particulièrement difficile de sortir de cette opposition entre approches optimistes et pessimistes des technologies de l’information.

des publications sur la cybersécurité restent axés sur les politiques publiques et la résolution de problèmes. Cela est encore plus vrai lorsqu'on examine les différentes théories qui nous permettent d'envisager les technologies de l'information sous un angle relatif à la sécurité. Cette section n'aura pas pour but de produire ou reproduire un inventaire exhaustif des publications concernées mais de questionner leurs effets sur l'appropriation de l'objet. Cette section a ainsi pour objectif de délier notre objet référent (sécurité de l'information) du langage « cyber » par l'étude de la réception de l'objet dans ces théories. Nous aurons recours à une approche thématique tentant d'inclure l'ensemble des approches qu'il nous aura été donné d'observer à l'exception de celles que nous venons d'évoquer pour faire le lien entre l'enjeux de la sécurité et le langage. Nous n'évoquerons pas plus avant les travaux qui s'inscrivent dans d'autres approches de la politique internationale pour limiter aux Relations Internationales.

A – Approches générales des technologies de l'information et Théories des Relations Internationales.

Concernant la thématique de la sécurité internationale, l'un des articles les plus complets est sans doute l'article de Johan Eriksson et Giacomo Giampiero en 2006.⁸⁸⁵ Pour élargir l'approche en dehors de la thématique de la sécurité, trois documents sont intéressants. Le premier est un article qui a été publié par Mary Manjikian en 2010.⁸⁸⁶ Le deuxième est une présentation de Robert Reardon et Nazli Choucri réalisée pour l'édition 2012 de la conférence de l'*International Studies Association* (ISA).⁸⁸⁷ L'étude la plus récente à ce jour est l'étude de

⁸⁸⁵ ERIKSSON Johan, et GIAMPIERO Giacomello, « The Information Revolution, Security, and International Relations : (IR)Relevant Theory ? » *International Political Science Review*, vol. 27, no. 3, 2006, pp. 221–244.

⁸⁸⁶ MANJIKIAN Mary. « From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. » *International Studies Quarterly*, vol. 54, no. 2, 2010, pp. 381–401.

⁸⁸⁷ REARDON Robert et CHOUCRI Nazli, « The Role of Cyberspace in International Relations: A View of the Literature », 53^{ème} Convention annuelle de l'ISA « Power, Principles, and Participation in the Global Information Age », San Diego, États-Unis, 1^{er} au 4 avril 2012.

Myriam Dunn Cavelty et Florian Egloff⁸⁸⁸. Du point de vue des ouvrages, nous retiendrons enfin l'introduction d'un ouvrage récent de Daniel McCarthy publié en 2018.⁸⁸⁹

De cette approche de la littérature ressort un paradoxe. D'un côté, il y a une insuffisance manifeste à penser la technologie dans les grandes théories des Relations Internationales. Cela prend corps dans le texte par la présence d'un déterminisme technique qui accompagnera le développement des Relations Internationales dans les courants dominants depuis les années 20 jusqu'à la fin des années 90. De l'autre côté, émerge une littérature spécialisée concentrée sur l'objet technique qui est pourtant victime de la fracture entre les différents courants. Ce paradoxe induit un statut assez particulier dans les débats de la dimension internationale et politique des technologies : d'un côté, certaines théories portent « trop » sur la composante technique des relations interétatiques (alors que celle-ci ne serait pas si importante que ça), de l'autre, la technique en tant que processus est un objet négligé. Il ressort une très grande spécialisation des textes qui étudient la technique qui renforce la difficulté de la conversation métathéorique.

1 – Le déterminisme technique inhérent au développement des Relations Internationales.

. Contrairement à l'idée reçue, la technologie et son caractère international sont présents au cœur des théories des Relations Internationales depuis le commencement de celles-ci. Ces éléments font le plus souvent figures de contexte voir de variable causale. La technologie reçoit un traitement inégal dans la plupart des grandes théories mais la thématique est présente. Pour Alfred Zimmern, la loi inexorable de l'intégration ne peut résulter à l'échelle internationale que de l'innovation technologique en ce qu'elle accroît la communication et le transport⁸⁹⁰. L'idée que ce changement poserait un grand défi à la souveraineté de l'État est présente chez Edward

⁸⁸⁸ Cette étude sur la cybersécurité est intéressante en ce qu'elle illustre qu'un certain nombre de problématiques soulevées dans cette section constituent toujours des domaines de friction, en particulier les libertés civiles. CAVELTY Myriam Dunn et EGLOFF Florian J. , « The Politics of Cybersecurity: Balancing Different Roles of the State. », *St Antony's International Review* vol. 15 no.1 , 2019, pp. 37-57.

⁸⁸⁹ MCCARTHY Daniel R., *Power, Information Technology, and International Relations Theory: the Power and Politics of US Foreign Policy and the Internet*. Palgrave Macmillan, 2015, 220 p. ; MCCARTHY, Daniel R. (dir), *Technology and World Politics an Introduction*. Routledge, Taylor & Francis Group, 2018., 272 p.

⁸⁹⁰ Voir l'article : ZIMMERN, Alfred, «The Prospects for Democracy ». *International Affairs* 7, 3, 1928, pp. 153–191. Voir plus spécifiquement p. 154.

Hallett Carr⁸⁹¹. Ce serait même l'un des plus grands changements qu'auraient à affronter les prochaines générations⁸⁹². De même chez Hans Morgenthau, la technologie impacte l'évolution de l'armement et donc oriente la stratégie militaire⁸⁹³. Le changement technologique doit se comprendre comme un facteur de force et d'influence dans les Relations Internationales⁸⁹⁴. Dans une première conception, la technique est une forme de déterminisme qui vient impacter l'objet d'analyse. L'idée de technique, se comprend ainsi comme de culture intégrée du progrès technique⁸⁹⁵, plutôt qu'un travail sur la technique en tant qu'objet scientifique.

Force est de constater que les auteurs semblent réticents à exclure ce déterminisme de la technique. Dès lors, l'univers conceptuel qui semblerait a priori le mieux correspondre à cette traduction est le constructivisme introduit dans les Relations Internationales par Alexander Wendt⁸⁹⁶. Néanmoins, ce constructivisme ne s'aurait qu'être critique voire radical pour intégrer une réelle dimension discursive sur la technique⁸⁹⁷... En effet, durant l'année 1999 dans sa critique du réalisme, Alexander Wendt s'il en avant met en le rôle des idées et des intérêts dans la constitution des relations internationales⁸⁹⁸, mobilise un fond matérialiste (« *rump materialism* ») pour son étude des relations internationales. Il affirme notamment que les forces matérielles brutes comme la force armée, les ressources naturelles ou la technologie possèdent un effet sur les politiques internationales. Il ajoute qu'un déterminisme technologique épuré (« *stripped down technological determinism* ») est compatible avec le constructivisme⁸⁹⁹.

⁸⁹¹ CARR Edward H. *The Twenty Years' Crisis, 1919–1939: An Introduction to the Study of International Relations*, Londres, Macmillan, 1939, 312 p.

⁸⁹² Ibid p. 295.

⁸⁹³ Par exemple, MORGENTHAU Hans,

⁸⁹⁴ Voir ici l'application de l'idée de structure et de mode de destruction chez DEUDNEY Daniel et IKENBERRY Gilford John. « The Nature and Sources of Liberal International Order. », *Review of International Studies*, vol. 25, no. 2, 1999, pp. 179–196.

⁸⁹⁵ Voir TAGUIEFF, op-cit.

⁸⁹⁶ La plupart des auteurs dont nous avons mobilisés les théories dans la première section de ce chapitre peuvent être d'ailleurs inscrit dans une forme de constructivisme.

⁸⁹⁷ Cf. chap. liminaire

⁸⁹⁸ Voir notamment les développements consacrés (pp. 254 – 257) dans l'ouvrage : WENDT Alexander, *Social Theory of International Politics*, Cambridge University Press, 1999, 429 p.

⁸⁹⁹ Ibid, pp 111 – 112. Cependant depuis lors Alexander Wendt est revenu sur cette assertion dans l'ouvrage WENDT, Alexander. *Quantum Mind and Social Science Unifying Physical and Social Ontology*, Cambridge University Press, 2015, 366 p.

Les deux exemples qui reviennent le plus lorsque l'on traite de technologies dans les Relations Internationales sont la dissuasion par l'arme nucléaire et justement les technologies de l'information. L'impact de l'arme nucléaire sur les Relations Internationales représente une forme d'héritage de l'inventaire des arsenaux militaires dans les études stratégiques. Cette étude de la technique constitue l'un des socles de l'étude du concept de puissance. La technique marque ici la croissance de la puissance militaire à la base du concept de dilemme de sécurité théorisé par John Herz⁹⁰⁰. En 1981, Kenneth Waltz décrit la lente prolifération de l'arme nucléaire dans un monde bipolaire comme la variable à l'aune de laquelle les puissances américaines et soviétiques peuvent mesurer leur puissance respective. Cette variable technique forgeant d'une part comme de l'autre un équilibre de la terreur indestructible⁹⁰¹. L'article va plus loin en évoquant les nombreuses raisons pour posséder une arme nucléaire sans toutefois décrire les politiques de création. Au travers de nombreuses études d'impact de l'arme nucléaire sur l'ordre mondial⁹⁰², les Relations Internationales ne se demandent pas vraiment comment ces technologies existent dans les différentes politiques qui président aux transformations dont elles ne sont qu'une variable. Paradoxalement, on pourrait ici souligner que la technologie est toujours une variable causale d'une politique et non pas un objet politique en elle-même.

Les technologies de l'information sont une thématique également décrite comme une variable qui va transformer le pouvoir à l'échelle mondiale (Ce serait également une des composantes principales du phénomène discursif « cyber »). En 1977, Joseph Nye et Robert Keohane placent les technologies comme source de la découverte de nouveaux espaces permettant d'en tirer des ressources, de même que les technologies de l'information et de la communication ont permis la diminution du coût de la distance⁹⁰³. Des lignes téléphoniques,

⁹⁰⁰ Voir HERZ, John H., « Idealist Internationalism and the Security Dilemma », *World Politics*, Vol. 2, N° 2, Janvier 1950, pp. 157–180

⁹⁰¹ WALTZ Kenneth, « The Spread of Nuclear Weapons: More May Better », *Adelphi Papers*, N° 171, 1981,

⁹⁰² Voir par exemple les travaux de Donald A. MacKenzie ou Joseph P. Masco: MACKENZIE Donald A. *Inventing Accuracy: a Historical Sociology of Nuclear Missile Guidance*. MIT Press, 2001, 478 p ; MASCO Joseph P. *The Nuclear Borderlands: The Manhattan Project in Post-Cold War New Mexico*, Paperback, janvier 2006, 448 p..

⁹⁰³ Parmi les exemples retenus dans l'ouvrage, on trouvait notamment le téléphone satellitaire. KEOHANE, Robert O. et NYE Joseph S.. *Power and Interdependence: World Politics in Transition*. Little, Brown and Company, 1977, 273 p.

les études aborderont beaucoup plus tard la question d'Internet puis des téléphones mobiles, de l'impression en trois dimensions ou de la réalité virtuelle.

Selon Daniel McCarthy⁹⁰⁴, le déterminisme technologique domine les Relations Internationales car il coïncide souvent avec une conception de la causalité dominante fondée sur la régularité⁹⁰⁵. De plus, les théoriciens des Relations Internationales n'ont pas classiquement recours à des approches historiques ou sociologiques des technologies, ce qui les entraînent vers une ontologie linéaire et contingente⁹⁰⁶. Et enfin, les paradigmes dominants des Relations Internationales ont le plus souvent fonctionné avec une compréhension positiviste de la connaissance.

2 – Impact des approches paradigmatisques des technologies de l'information.

Une question fondamentale demeure puisque nous cherchons à recourir à une combinaison pragmatique entre plusieurs théories. Comment les paradigmes des Relations Internationales influencent-ils la perception de la technologie comme objet d'étude dans le contexte de l'émergence des technologies de l'information ? Afin d'y répondre, nous nous concentrerons sur les trois grandes approches dominantes que sont le réalisme, le libéralisme et le constructivisme⁹⁰⁷.

S'inscrire dans le courant réaliste, du point de vue des technologies de l'information c'est parler majoritairement de la sécurité et parfois de gouvernance⁹⁰⁸. Mais le courant réaliste et les hypothèses qui le constituent sont en proie à un dilemme de la part des chercheurs. Pourquoi les technologies de l'information seraient-elles si importantes que ça ? Plus précisément, pourquoi faudrait-il prendre en compte cette dimension d'un point de vue

⁹⁰⁴ MCCARTHY Daniel R. (dir), 2018, op-cit., pp. 9-11.

⁹⁰⁵ KURKI Milja, 2008, op-cit. ; KURKI Milja et WIGHT, Colin, 2013, op-cit.

⁹⁰⁶ BUZAN Barry, LITTLE Richard, et JONES Charles, *The Logic of Anarchy: Neorealism and Structural Realism*. New York, Columbia University Press, 1993, 267 p. ainsi que BUZAN Barry & LITTLE Richard, *International Systems in World History: Remaking the Study of International Relations*, Oxford University Press, 2001, 476 p.

⁹⁰⁷ Nous envisagerons les approches tirées de la sociologie comme un moyen de remettre en cause le déterminisme technique des Relations Internationales dans notre chapitre 5.

⁹⁰⁸ Nous aurons l'occasion d'y revenir en abordant l'article de Daniel Drezner. DREZNER Daniel W., « The Global Governance of the Internet: Bringing the State Back In », *Political Science Quarterly*, vol. 199 n°3, 2004, pp. 477-498.

théorique dans la mesure où cela ne bouleverse pas le système international et la sécurité militaire de l'État ? A priori, une vision traditionnaliste du réalisme qui confinerait presque à la caricature n'implique pas le besoin d'opérer un renouvellement d'un point de vue théorique⁹⁰⁹. Par rapport aux menaces consacrées par le discours que nous avons mis en évidence lors de la première partie de cette thèse, une telle approche envisagerait la sécurité de l'information comme un problème de nature économique qui n'est pas un objet de Relations Internationales au sens strict. Le réalisme peut-il intégrer une dimension économique afin d'élargir sa vision de la sécurité ? C'est ce qui résume la plupart des oppositions réalistes traditionnelles autour de la question des technologies de l'information. Dans une approche moins traditionnaliste, il est possible de trouver des théoriciens d'inspiration réalistes qui considèrent que la guerre de l'information est une nouvelle composante à part entière dans un conflit interétatique par ailleurs « traditionnel ». Parmi les travaux les moins récents, il est possible de citer par exemple les travaux de David Lonsdale en 1999⁹¹⁰. Lequel mobilise notamment la notion d'infosphère, à travers laquelle et à l'intérieur de laquelle, il est possible de projeter une forme de puissance stratégique. Particulièrement flexible, ce pouvoir de l'information donne aux acteurs non-étatiques les moyens d'agir sur la sphère internationale. Conséquence de sa flexibilité, de son omniprésence et de son accessibilité, il est difficile d'imaginer un acteur stratégique performant au XXIe siècle sans comprendre et prendre en compte le pouvoir de l'information⁹¹¹. On pourrait assister ici à un exemple de convergence entre (néo)libéralisme et (néo)réalisme sur le risque de déclin du pouvoir de l'acteur régional. Néanmoins, d'un point de vue réaliste, le numérique implique une part de technologie nouvelle et une capacité globale des adversaires renforcée, mais « les notions de base d'attaque et de défense de l'information et des systèmes d'information sont aussi anciennes que la guerre elle-même ».

A priori, une approche d'inspiration libérale a plus de facilités à penser l'objet des technologies de l'information. En effet, dans la plupart des lectures libérales de la politique mondiale contemporaine, il est avancé que la souveraineté de l'État-nation est en train d'être imprégnée et fragmentée par le développement de relations transnationales (et non pas

⁹⁰⁹ MANJIKIAN 2010, op-cit., pp. 384 -387.

⁹¹⁰ LONSDALE David J. « Information Power: Strategy, Geopolitics, and the Fifth Dimension. » *Journal of Strategic Studies*, vol. 22, no. 2-3, 1999, pp. 137–157.

⁹¹¹ Ibid. p. 154.

nécessairement par des adversaires mieux armés). D'ailleurs certains théoriciens libéraux vont même jusqu'à affirmer que la souveraineté est plus une sorte de fardeau qu'un véritable pouvoir⁹¹². Sans forcément ouvrir le débat sur la souveraineté, assez contre-intuitivement nous pouvons noter que peu de théoriciens libéraux se sont consacrés aux technologies de l'information de manière générale. Parmi les théories libérales, nous retiendrons ici le rôle particulier de l'institutionnalisme néo-libéral (ou transnationalisme) avec le travail de Keohane et Nye⁹¹³. De manière générale, la technologie est perçue comme quelque chose de positif au sein de la globalisation. Toutefois, les cybermenaces pourront être regardées comme des éléments de cette globalisation qui affaiblit la souveraineté de l'État et entraîne une pluralité d'acteurs non-étatiques croissante qui devient plus puissante. Les relations internationales apparaissent comme fluidifiées par les technologies de l'information permettant une meilleure intégration et une meilleure coopération ; tout autant que la déstabilisation des États, le crime international et le terrorisme apparaissent comme renforcés. Nous retiendrons du courant libéral pour les technologies de l'information : sa contribution à la prise en compte des acteurs nouveaux au sein de la gouvernance, sa réflexion le développement, son étude des régimes autoritaires et sa contribution au concept de cyberpower.

Le constructivisme pose davantage de questions dans la mesure où il se décline en plusieurs courants plus ou moins critiques avec des approches méthodologiques se revendiquant comme étant différentes les unes des autres. Nous retrouverons de nombreuses théories dont certaines ont déjà dû être mobilisées dans les premiers développements de cette thèse à l'image des communautés épistémiques qui s'inscrivent dans ce courant, ou encore de la lecture que nous avons de la théorie de la sécurisation. C'est un courant très hétérogène. Il se voit d'ailleurs disputé cette appellation⁹¹⁴. Si l'on devait trouver un trait commun aux approches constructivistes des technologies de l'information, il faut sans doute mettre en avant que ces

⁹¹² Voir en particulier la distinction « sovereignty-bound » / « sovereignty-free » chez James Rosenau. ROSENAU James N. *Turbulence in World Politics: a Theory of Change and Continuity*. Princeton University Press, 1990. 480 p. ainsi que pour les technologies de l'information l'ouvrage collectif précité ROSENAU, James N., et SINGH J. P. (eds), 2002, op-cit.

⁹¹³ Pour les premiers travaux voir KEOHANE, Robert Owen et NYE Joseph S., *Power and Interdependence: World Politics in Transition*. Boston, Little, Brown, 1977, 273 p. Ainsi que KEOHANE, Robert Owen et NYE Joseph S., *Power and Interdependence*, New York, Harper Collins, 1989. Pour la première application aux technologies de l'information, voir l'article KEOHANE, Robert Owen et NYE Joseph S., « Power and Interdependence in the Information Age. » *Foreign Affairs*, vol. 77, no. 5, 1998, p. 81 – 94.

⁹¹⁴ Cf. chapitre liminaire.

études soulignent la construction de l’identité et la signification des images et des symboles en plus de la réalité factuelle des ordinateurs et des câbles sous-marins, principaux vecteurs d’Internet. Il y a des études constructivistes qui s’intéresse uniquement à la sécurité, il y a des études qui s’intéressent aux technologies de l’information en elles-mêmes⁹¹⁵. Il y a enfin des approches qui croisent ces deux thématiques. Nous retiendrons donc en plus des approches dédiées à la sécurité que nous avons évoquées, l’apport constructiviste sur la gouvernance ainsi que la société civile globale. Il faut souligner que les articles d’inspiration constructivistes apparaissent comme majoritaire sur l’ensemble des thématiques qui s’intéresse à la sécurité de l’information. Les théories réalistes des relations internationales s’appliquent le mieux aux questions liées à la cybersécurité et à la cyberguerre. En effet, les théories réalistes peuvent aider à expliquer comment les États utilisent les technologies de l’information à des fins sécuritaires ou par maximiser leurs intérêts. Néanmoins, parce qu’ils cherchent à dépasser le déterminisme matériel de cette sécurité, les constructivistes peuvent s’intéresser à des objets plus nombreux et ne souffrent pas du fait de voir leurs hypothèses mises en danger par l’émergence de nouveaux acteurs.

3 – Récits et conceptualisations du cyberespace dans les Relations Internationales.

Une dernière brique nous manque avant d’aborder thématiquement la réception des discours de sécurité de l’information dans les Relations Internationales. A cet instant, nous avons notre analyse du phénomène linguistique « cyber » qui constitue la première partie de cette thèse. Nous pouvons cerner la transformation à l’échelle politique de l’information en enjeux de sécurité dans divers domaines grâce à la sécurisation. Cette dernière transformation est par ailleurs complétée d’un important travail sur la circulation de l’idée par le biais des acteurs scientifiques. Par ailleurs, nous pouvons analyser ce processus comme la prise en compte d’une sécurité de l’information qui existe en dehors des seuls discours analysés. Cette sécurité de l’information éclaire plus largement les compréhensions des technologies de l’information. Ce qu’il nous manque c’est l’influence du cyberespace en tant que récit chez les théoriciens des Relations Internationales. Cette influence est importante à prendre en compte lorsqu’elle implique des conséquences conceptuelles et métathéoriques sur les objets d’analyse. Nous soutenons que le phénomène du cyberespace et des termes dérivés ne fait pas l’objet d’une

⁹¹⁵ HERRERA Geoffrey L. « Technology and International Systems. » *Millennium*, vol. 32, no. 3, décembre 2003, pp. 559–593.

réception neutre dans les différentes théories des Relations Internationales et qu'il existe différents biais qu'il faut indiquer avant d'examiner plus avant le contexte d'emploi de la sécurité de l'information dans la littérature. Cette précaution est d'autant plus nécessaire que les travaux de recherche sur la sécurité de l'information se distinguent par les objets et ne permettent pas de les distinguer par les discours.

Le travail le plus éclairant réalisé sur cette question particulière de la perception du cyberespace en tant que récit est sans nul doute la discussion autour des visions libérales et réalistes du cyberespace proposée par Mary Manjikian en 2010⁹¹⁶. Le but de cet article particulier n'est pas forcément de discriminer entre la bonne théorie et la mauvaise théorie, mais de souligner la différence de perception d'un objet selon le courant dans lequel un chercheur cherche à s'inscrire. Son travail s'articule autour de la différence entre l'image du village global (libérale) et l'espace de bataille virtuel (réaliste).

« Le cyberespace est soit un espace et un lieu qui offre un potentiel de libération personnelle, la création de structures de coopération internationale et une plus grande mobilisation et participation des citoyens ; ou bien c'est une extension sombre et sinistre de certaines des parties les plus dangereuses et non gouvernées de notre monde physique, un nouveau type d'espace défaillant avec le potentiel de générer des menaces réelles qui se répercuteront rapidement dans le monde réel. »⁹¹⁷

Ce que nous analysions précédemment du point de vue du discours trouve donc sa traduction presque littérale dans les théories des Relations Internationales. Mary Manjikian aboutit dans son travail à différencier trois grandes postures pour conceptualiser le cyberespace : utopique (*utopian*), réglementaire (*regulatory*) et réaliste (*realist*)⁹¹⁸. Chacune de ces postures renvoie à des conceptions différentes du territoire, du pouvoir, de l'identité⁹¹⁹, de la crédibilité de l'acteur régaliens, de l'information, de régulation et de la croissance de celle-ci. Lesquelles ont une incidence sur les contours du concept final et sur les postulats de départ des études.

⁹¹⁶ MANJIKIAN Mary, 2010, op-cit.

⁹¹⁷ Ibid. p. 398.

⁹¹⁸ Ibid. p. 387.

⁹¹⁹ Assimilé à la nationalité dans le cadre de cet article.

Dans une optique utopique, le cyberespace apparaît comme extraterritorial. Il n'y a pas de voisinage donc aucune frontière. Le monde virtuel et le monde réel sont strictement séparés. Par analogie, on pourra comparer le cyberespace à une métaphore numérique de l'espace au sens cosmologique (*Outer Space*). Le pouvoir lié à ce cyberespace agit pour subvertir les structures existantes. Dès lors, l'identité est désincarnée. Le citoyen est avant tout un utilisateur d'Internet, anonyme et pour qui la nationalité n'a pas d'importance. La crédibilité de l'acteur régional dans ce système est sans importance voire sans rapport avec le sujet. L'information quant à elle est partagée et infinie. La régulation s'établit sur la base de principes éthiques et de normes communautaires dont la croissance est perçue comme organique et autoproduite par les communautés.

Dans une optique réglementaire, le cyberespace est considéré comme un territoire international. La frontière y est présente mais n'est pas fixe. Ici, l'analogie qui convient le mieux est celle de l'océan. Dans ce modèle, le cyberespace récupère et reproduit les structures de pouvoir existantes. L'identité numérique correspond à la digitalisation des personnes et est compatible avec l'idée de nationalité. L'État demeure le principal agent et doit créer de la confiance. L'information est libre. Elle fait partie des biens communs et s'inscrit dans une recherche d'ouverture la plus large possible⁹²⁰. La régulation est à la fois déterminée par la loi du marché et par les États. La croissance de celle-ci est principalement le fruit d'une « *lex informatica* » créée dans un dialogue entre l'expertise informatique et les processus sociaux.

Le dernier modèle est l'approche « réaliste ». Dans cette approche, le cyberespace est un lieu externe où s'applique le pouvoir du monde réel. Ce lieu implique de la propriété, des frontières, des sanctuaires, un « Dark Web » et des Pare-feu. Ce lieu est géré et attribué de manière centralisée. Et il existe des effets d'entraînement du monde virtuel vers le monde réel. De manière générale, Internet fait partie de la construction des nations. Le citoyen y représente un individu à protéger. La crédibilité de l'État passe par l'idée qu'il est protecteur et que cette protection est bénéfique sinon souhaitable. L'information est un bien qui est susceptible d'appropriation. Elle est également une arme dans le cadre des combats pour assurer le territoire et la crédibilité de l'acteur régional, qu'elle soit employée pour des frappes informatiques ou à des fins de guerre des idées.

⁹²⁰ Que l'auteure rapproche des mouvements d'ouverture type *Open Data*, *Open Gov*, *Open Source*, etc.

Sur la question du territoire, la grande division consiste dans le sens de la dichotomie entre monde réel et monde virtuel. D'un côté, les optiques utopique et réglementaire considèrent cet espace comme étranger par nature aux formes politiques antérieures. Alors, que de l'autre côté, les réalistes vont considérer cet espace virtuel comme le prolongement du monde réel. Cela entraîne deux visions du monde virtuel : l'une, où il est approprié voire « colonisé » ; l'autre où il n'est pas gouverné et où il est peut-être même ingouvernable.

La grande division dans la considération de l'individu repose sur la réception de la capacité de mobilisation de nombreux individus sur de larges territoires ainsi que de nouveaux acteurs. Si on regarde le modèle utopique, chaque citoyen d'Internet a théoriquement la même capacité de mobilisation et de réalisation d'objectifs personnels et collectifs, ainsi que la capacité de mobilisation des autres citoyens grâce à la disparition du pouvoir et des normes du monde physiques. D'un point de vue réglementaire libéral, les citoyens assimilent les normes et les comportements de la communauté tout en travaillent pour préserver les biens collectifs. Il y a donc des limitations à la capacité de mobilisation des citoyens qui sont liées aux frontières du cyberspace, aux contextes nationaux dont ils dépendent et aux normes internationales. D'un point de vue réaliste, le cyberspace permet la mobilisation de bons citoyens qui acceptent les règles et de mauvais qui les refusent. Le cyberspace agit comme un refuge qui abrite et cultive les « insurgés ». Ces derniers bénéficient d'un Internet qui brouillent les frontières entre non combattants et combattants et qui aide à développer une identité virtuelle communautaire non-étatique.

Enfin, ces trois modèles se divisent sur leurs représentations de l'information. L'information libre se concrétise dans la convergence de tous les médias et moyens de communication vers Internet ainsi que par la neutralité de ce dernier. L'information comme bien commun suppose des moyens normatifs et institutionnels visant à assurer la qualité et la disponibilité de l'information. Par ailleurs, les inégalités économiques et politiques récurrentes à l'échelle du globe atténuent l'idéal de la libre circulation de l'information. L'information appropriable suppose une forme d'exclusivité qui fait naître un certain nombre d'avantages. C'est tout l'enjeu de la menace perçue dans une optique réaliste qui se décline en logique compétitive autour de la guerre de l'information, la course aux armements de l'information, et enfin sur les vulnérabilités de réseaux à la fois technique et humains. L'information n'est pas libre (quand bien même elle ne peut pas être maîtrisée), elle ne peut pas faire l'objet de

régulation (quand bien même on peut se l'approprier), mais elle est le terrain non seulement du conflit armé mais en plus de conflits idéologiques.

Il y a donc des différences fondamentales dans la manière de conceptualiser le cyberespace qui constituent autant de métarécits qui viennent alimenter une certaine vision du monde concernant les recherches sur les technologies de l'information qui mobilisent le cyberespace en tant que concept. Ces récits apparaissent comme la transcription d'une approche « technophile / technophobe » mais ne présage pas *a priori* d'une vision techno-centrée. On peut en déduire qu'il n'y pas de différence suffisamment marquée entre les modèles sur ce point. Du point de vue des points communs, on observe un postulat dichotomique entre l'information numérisée et la réalité. La reconnaissance commune d'une faculté de mobilisation au travers d'Internet. Enfin, on retrouve l'idée d'un dépassement de la perception humaine par rapport à l'information.

B – La technologie et la sécurité, entre influence normative et partage du pouvoir.

Notre approche visera ici à interroger plus spécieusement la représentation de la sécurité dans les approches des technologies de l'information dans les normes internationales. Nous aborderons en particulier la littérature qui concerne le sujet de la gouvernance d'Internet, la globalisation, la théorie du *cyberpower*, les théories du développement ainsi que l'impact des technologies sur les régimes autoritaires. Lesquelles revoient à des problématiques liées aux acteurs des Relations Internationales. C'est sans doute le premier point à retenir : les théories des Relations Internationales prises de manière isolées n'ont pas nécessairement les outils ou les travaux capables d'intégrer l'ensemble des phénomènes. Parmi les exemples les plus saillants, on retrouve le faible traitement de la criminalité informatique qui est pourtant l'un des terrains où les relations sont en pratique les plus construites entre les acteurs.

Dès lors, les chercheurs qui veulent travailler sur la technologie, ou plus exactement sur le fait de savoir étudier comment naissent les objets technologiques, leur rôle leur compréhension, doivent recourir aux apports d'autres disciplines que les Relations Internationales. Si on se limite au périmètre de cette recherche, il est possible de citer les quelques apports de la philosophie de la technique, de la philosophie des sciences, de la

sociologie des sciences et des techniques, de la sociolinguistique⁹²¹... La plupart des travaux de recherche consacrés à un objet technologique font appel à des méthodes hybrides ou à des approches pluridisciplinaires. Cela détache cette production scientifique des approches générales pour en faire des travaux de recherche spécialisés dont les apports se limitent souvent à la compréhension d'un objet (par exemple la sécurité) plutôt que directement la dimension internationale du politique. Dans la perspective des Relations Internationales, cela cantonne majoritairement la place de la technologie à certains « débats sectoriels ». La littérature sur le cyberespace ou les technologies de l'information souffre également d'un manque d'études empiriques. De trop nombreux ouvrages ou articles apparaissent comme des études abstraites ou des essais.

Si la sécurité est une thématique relativement présente dans la littérature, on remarquera que celle-ci est ambivalente selon les théories mobilisées. Par exemple les auteurs critiques de la société civile globale auront par exemple tendance à voir la recherche de sécurité comme la domination des impératifs commerciaux sur l'architecture d'Internet. Tandis que les débats autour de la gouvernance d'Internet traiteront la sécurité comme étant soit l'objectif de la sécurité du citoyen au travers de la protection de ses droits fondamentaux.

1 – Gouvernance et Internet : un modèle de participation ?

Nous avons déjà évoqué la question complexe de la gouvernance d'Internet et les enjeux qui structurent une partie de sa remise en question⁹²². Internet constitue un mode original de gouvernance contestée entre divers acteurs internationaux. Là où Internet se distingue d'autres grands ensembles politiques, tels l'Organisation des Nations Unies, c'est par la complexité et la diversité des acteurs qu'elle mobilise en tant que processus international. Par ailleurs, elle se caractérise par le fait qu'elle produit directement et techniquement de la sécurité. La plupart des articles de recherche ou des ouvrages consacrés à cette question ont pour but de discuter des modèles de gouvernance internationale capable de prendre en compte les intérêts de cette multitude ainsi que sur la manière dont Internet devrait être structuré et réglementé. La thématique de la gouvernance est l'une des thématiques les plus répandues. Du point de vue des Relations Internationales, Internet semble ainsi apparaître comme un laboratoire de test

⁹²¹ Nous aurons l'occasion d'aborder certaines de ces approches au moment de notre chapitre 5.

⁹²² Cf. Chapitre 3.

construit pour traiter du « troisième grand débat inter-paradigmatique » entre les approches centrées sur l’État et leurs critiques. Dans l’ensemble des approches, se retrouve néanmoins un souci de prise en compte de la diversité des parties prenantes.

Dans une optique d’inspiration réaliste, on peut faire référence à l’approche de Daniel Drezner formulée en 2004⁹²³. Le postulat de Drezner s’articule autour de la durabilité et de la délégation. Pour contrer l’idée selon laquelle la globalisation et Internet affaiblissent la capacité de l’acteur régional à gouverner l’économie mondiale, l’auteur va mobiliser la capacité des États à substituer différentes structures de gouvernance et différents outils politiques pour créer ces structures, en fonction de la constellation de leurs intérêts⁹²⁴. Un État surtout s’il est une « grande puissance » est ici capable de déléguer à des acteurs non-étatiques, de créer des régimes internationaux avec une infrastructure lourde et de multiplier ces régimes et ces délégations afin de créer la concurrence nécessaire au bon fonctionnement de l’ensemble. Par ces mécanismes, les enjeux de la gouvernance d’Internet sont rationnellement déterminés par les États les plus puissants.

« Le pouvoir de l’État est défini comme la taille du marché intérieur d’un État ; plus le marché est grand, plus l’État est puissant. Les États dotés de marchés intérieurs importants sont moins dépendants des échanges internationaux en tant que source de biens et de capitaux. »⁹²⁵

Afin d’enrichir ce premier postulat, Drezner ajoute que la gouvernance d’Internet n’est pas unidimensionnelle mais s’attache au contraire à plusieurs déclanisons que sont par exemple l’élaboration de protocoles techniques, la censure, la taxation électronique, la propriété intellectuelle et les droits à la vie privée où les intérêts de chaque État ne sont pas forcément identiques⁹²⁶.

« [...] Leurs préférences en matière de réglementation ont leur origine dans la politique intérieure. [...] la plupart des problèmes sociaux ont leur origine dans les problèmes nationaux avant que la mondialisation n’en fasse des problèmes internationaux. Les gouvernements préféreront naturellement que les réglementations mondiales reflètent leurs propres normes nationales. Cela réduit les coûts

⁹²³ DREZNER Daniel., 2004 op-cit.

⁹²⁴ Ibid. p. 478.

⁹²⁵ Ibid. p. 482. (Notre traduction)

⁹²⁶ Ibid. p. 479.

d'ajustement de tout changement législatif ou réglementaire requis pour les gouvernements, ainsi que les coûts pour les entreprises nationales de se conformer à une nouvelle norme. »⁹²⁷

Il en ressort deux avantages pour l'État : l'obtention éventuelle d'un avantage du fait de sa conformité au standard internationale et la diminution de l'insécurité juridique pour ses citoyens⁹²⁸. Il est dès lors possible de classer les enjeux de la gouvernance en fonction du degré de conflictualité entre les États les plus puissants, puis entre eux (Nord) et les États marginaux (Sud). Si le conflit est présent de toute part, la gouvernance se concentrera sur la censure (*Sham standards*). Si le conflit est présent entre États puissants et marginaux mais qu'il est moins important entre les puissants (*Club standards*), la gouvernance se concentrera sur la propriété intellectuelle. Si c'est la situation inverse qui se produit (*Rival standards*), la gouvernance sera focalisée sur la vie privée. Et enfin en cas de conflit bas de toute part (*Harmonized standards*), la gouvernance se concentrera sur les protocoles techniques⁹²⁹. A l'aide des exemples de l'ICANN, de la protection des données dans l'Union Européenne, ou des accords internationaux sur la propriété intellectuelle, cette typologie permet à l'auteur d'argumenter sur une erreur de la littérature dédiée à la gouvernance d'Internet en Relations Internationales en ce qu'elle méconnait la primauté de l'État ainsi que la diversité des relations qui peuvent exister entre des acteurs hétérogènes de la politique internationale⁹³⁰.

L'ICANN, l'Union Européenne ou les accords concernant la propriété intellectuelle font également partie des exemples retenus par les auteurs d'inspiration libérale pour mettre l'accent l'importance du rôle des acteurs non-étatiques dans la gouvernance d'Internet. Ainsi le fait que l'Union Européenne ait été l'une des premières institutions internationales à prendre une directive sur la protection des données personnelles en 1995⁹³¹ est un exemple tantôt mobilisé par les réalistes, tantôt par les libéraux en fonction de l'acteur considéré ou selon que l'article portera sur la régulation du commerce ou sur la protection des libertés civiles liées à Internet.

⁹²⁷ Ibid. p. 482. (Notre traduction)

⁹²⁸ Même si l'auteur se concentre avant tout sur l'entreprise.

⁹²⁹ Ibid. p. 483.

⁹³⁰ Ibid. p. 498.

⁹³¹ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogée le 25 mai 2018.

C'est notamment le cas en 2008 avec l'article d'Abraham Newman consacré aux entrepreneurs transgouvernementaux (*transgovernmental policy entrepreneurs*)⁹³².

L'article se fonde sur l'adoption de cette norme et deux éléments factuels : d'une part, la pluralité d'acteurs entre États, industrie et commission européenne directement concernés par le processus d'élaboration de la norme ; d'autre part, l'échec des deux grandes théories de l'intégration européenne que sont l'intergouvernementalisme libéral et le néofonctionnalisme dont les « protagonistes » se sont opposés sur la question de la directive⁹³³. Cela permet à Abraham Newman de dégager le rôle moteur d'un autre type d'acteur dans la politique publique européenne. Dans ce contexte, les autorités nationales dédiées à la protection des données personnelles créées par des législations nationales antérieures ont poussé à l'adoption de règles internationales visant la protection des données personnelles et de la vie privée. Les différentes autorités nationales ont utilisé leur expertise pour définir un programme politique supranational. Elles ont également employé la puissance normative reçue par délégation des États pour bloquer les connections et les transferts de données vers les pays dépourvus de législation ou avec une législation laxiste. Cela concerne notamment la Belgique, l'Espagne, le Portugal, l'Italie et la Grèce qui ne disposaient d'aucune législation antérieure sur la protection des données à l'époque. En agissant de la sorte, ces institutions ont modifié l'analyse coûts-avantages des décideurs supranationaux et ont fait pression sur la commission et les États membres en faveur de l'harmonisation européenne de la protection des données personnelles.

Si l'on s'attarde sur le concept de *Transgovernmental Policy Entrepreneur* qui est dégagé dans l'article, il ressemble essentiellement à celui de communauté épistémique mais s'en distingue par son aspect « entrepreneurial ». L'acteur ne se contente pas d'influencer la prise de décision mais mobilise son pouvoir pour imposer ses préférences. Ce pouvoir procède principalement de la réunion de trois éléments : l'expertise technique comme outil de formulation des problèmes et des solutions politiques, la délégation interne d'autorité reçue de

⁹³² NEWMAN Abraham L. « Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive. », *International Organization*, vol. 62, no. 01, 2008, pp. 103 – 130. Il s'agit pour partie d'une reprise de travaux antérieurs de l'auteur ayant fait l'objet d'une présentation en août 2003 au congrès annuel de l'*American Political Science Association*. Pour une version actualisée de cette théorie, voir NEWMAN, Abraham L. *Protectors of Privacy: Regulating Personal Data in the Global Economy*, Ithaca, Cornell University Press, juillet. 2018, 240 pages

⁹³³ Ibid. p. 105.

l'acteur régalien et le réseau transnational qui relie chacune des institutions concernées et qui est constitutif de l'acteur⁹³⁴. Il a néanmoins un fossé entre cette étude et l'idée d'une gouvernance globale d'Internet qui pose la question de sa transposition possible. Une piste est sans doute à rechercher du côté des CERTs pour voir si en dehors de leur caractère de communauté épistémique, ces derniers peuvent également initier et imposer une harmonisation de la règlementation sur des questions de gouvernance d'Internet dans un cadre multilatéral différent de l'Union Européenne⁹³⁵. De telles recherches n'ont pas encore donné lieu à publication.

Dans une logique identique à celle de Dresden sur la place prépondérante des acteurs régaliens, nous retrouvons les travaux d'Henry Farrel qui mobilisent une approche constructiviste afin d'analyser les processus de négociation relatifs aux accords dit de la « sphère de sécurité » (*Safe Harbor*) mise en place entre les États-Unis et l'Union Européenne entre 1998 et 2000 suite à la directive de 1995⁹³⁶ ⁹³⁷. Cet accord avait pour but de réglementer les échanges transatlantiques de données à caractère personnel à des fins commerciales⁹³⁸. Le rôle de l'approche constructiviste est ici de mettre en avant la controverse des acteurs afin d'éclairer le résultat final du processus de négociation. La controverse se produit théoriquement lorsque les acteurs ont des visions diamétralement opposées mais où il existe une incertitude à long terme sur les résultats des actions entreprises. Cette configuration facilite la persuasion et donc la négociation⁹³⁹. Il en résulte que l'exemple de la Sphère de sécurité invalide l'hypothèse selon laquelle les acteurs privés prennent le devant de la scène dans la gouvernance du commerce électronique. Bien que les acteurs privés jouent un rôle important dans la

⁹³⁴ Ibid. p. 119-126.

⁹³⁵ Sur la question des CERTs, cf. chapitre 3.

⁹³⁶ *Décision 2000/520/CE* de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique

⁹³⁷ FARRELL Henry, « Constructing the International Foundations of E-Commerce : The EU-US Safe Harbor Agreement », *International Organization*, vol. 57 n°2, 2003, pp. 277-306.

⁹³⁸ Il a été remplacé en 2016 par un nouvel accord : le « Bouclier de protection des données UE-États-Unis ».

⁹³⁹ RISSE, Thomas. « Let's Argue!': Communicative Action in World Politics. » *International Organisazation*, vol. 54, n°1 2000, pp 1-41.

gouvernance d'Internet notamment sur le volet de la vie privée, c'est en grande partie dû à l'action de l'État.

« L'histoire de la sphère de sécurité suggère que les accords hybrides ont leur origine dans l'interdépendance croissante à laquelle le commerce électronique donne naissance. [...] Lorsque les différences d'approche réglementaire reflètent des conflits plus profonds sur les principes sous-jacents de l'ordre social, ces problèmes sont difficiles à résoudre par la négociation conventionnelle. [...] L'UE et les États-Unis ont donc cherché à créer un mécanisme d'interface permettant d'atténuer les problèmes d'interdépendance. »⁹⁴⁰

Une dernière façon d'étudier la gouvernance est d'utiliser pour déterminer jusqu'à quel point Internet est ouvert et peut réellement constituer un bien commun. C'est notamment l'approche critique de Lawrence Lessig sur la propriété intellectuelle et Internet⁹⁴¹. La critique majeure de Lessig se focalise sur la distinction entre la plateforme qu'Internet était censé être à l'origine et la fermeture induite par les nouvelles normes en matière de droit informatique et de propriété intellectuelle (notamment en matière logicielle) qui s'opposent à l'idée de bien commun sur le long terme. Il en résulte des réglementations allant à l'encontre du développement et de la croissance à l'échelle globale qui défavorisent les États les moins puissants sur la scène internationale⁹⁴². L'architecture d'Internet ne devait pas être considérée comme acquise. Dans cette approche la pratique de la gouvernance s'oppose aux libertés⁹⁴³. De ce point de vue, beaucoup de ces idées reçues sur le caractère ouvert et libéral d'Internet et ses nombreuses conséquences sont moins révélatrices de la nature de la technologie que des propriétés de son contexte d'emploi.

Pour aller plus loin dans la thématique de la gouvernance et de la sécurité de l'information, le concept de bien commun est un outil assez utile pour examiner la manière dont

⁹⁴⁰ FARRELL Henry, 2003, p. 300 (notre traduction).

⁹⁴¹ Voir LESSI, Lawrence, *Code and Other Laws of Cyberspace*. Basic Books, 1999, 320 p. ; ainsi qu'en particulier LESSIG Lawrence, *The Future of Ideas: the Fate of the Commons in a Connected World*. Random House, 2001, 297 p.

⁹⁴² Sur les différents modes de contrôle d'Internet, voir la partie 3 de l'ouvrage LESSIG Lawrence, 2001, pp 149 – 262.

⁹⁴³ Il y a des approches plus favorables à la gouvernance concernant le statut de bien commun d'Internet. Voir en particulier CUKIER, Kenneth Neil. « Who Will Control the Internet? Washington Battles the World. » *Foreign Affairs*, vol. 84, no. 6, 2005, p. 7- 13 ou encore BAIRD Zoë. « Governing the Internet: Engaging Government, Business, and Nonprofits. », *Foreign Affairs*, vol. 81, no. 6, 2002, p. 15 - 20.

se construit une partie des échanges internationaux autour du numérique. Dans un long article tiré de ses travaux de thèse⁹⁴⁴, Scott Shackelford mobilise les exemples des modèles de gouvernance de l'ICANN, de l'IETF et de l'UIT afin de mesurer leur impact en termes de sécurité et de gouvernance globale d'Internet au travers d'une analyse polycentrique où plusieurs centres de décision formellement indépendants concourent à la prise de décisions⁹⁴⁵.

Parmi les principales conclusions de cet article, la notion d'une implication minimale du gouvernement national dans la gouvernance de l'Internet semble devoir être contestée. À l'heure actuelle, le cyberespace est un mélange de lois non contraignantes (*soft law*), de réglementations nationales, d'accords régionaux, de droit international coutumier et de traités multilatéraux, mais aucun d'entre eux n'a le pouvoir ou le mandat de gérer l'intégralité d'Internet. Si l'IETF, pour sa part, peut être considéré comme un modèle de système polycentrique performant, grâce à la publication croissante de normes pour la gouvernance d'Internet, elle n'a cependant pas réussi à imposer largement et à mettre en œuvre des protocoles sécurisés.

Malgré la théorisation de la cyberpaix, pour l'auteur les parties prenantes doivent reconnaître que celle-ci nécessite non seulement de résoudre la cyberguerre, mais également la cybercriminalité, le cyberterrorisme et le cyberespionnage. Les États peuvent toutefois entamer un processus de limitation de l'escalade de la cyberguerre par l'élaboration de normes en groupe restreint. L'article propose enfin des « initiatives polycentriques » destinées à faciliter la mise en place d'une gouvernance globale d'Internet avec ou malgré la cybermane.

« Premièrement, les alliés devraient travailler ensemble pour élaborer un code de conduite commun incluant des normes de base, notamment pour ne pas limiter indûment certaines libertés de l'Internet, pendant que les négociations se poursuivent sur un cadre juridique mondial harmonisé. Deuxièmement, les gouvernements et les opérateurs devraient établir des politiques de cybersécurité complètes et

⁹⁴⁴ SHACKELFORD Scott J., « Toward Cyberpeace: Managing Cyberattacksthrough Polycentric Governance », *American University Law Review*, vol 62, n°5, 2013, pp. 1273 – 1364Ainsi que la thèse : SHACKELFORD Scott J., *Governing the Global Commons in International Law and Relations* Université de Cambridge, 15 Nov, 2011. Voir également l'ouvrage plus récent : SHACKELFORD, Scott J.. *Managing Cyber Attacks in International Law, Business, and Relations: in Search of Cyber Peace*. Cambridge Univ Press, 2016, 434 p.

⁹⁴⁵ Concept inspiré des travaux d'Elinor Ostrom. OSTROM Elinor, *La Gouvernance des biens communs : Pour une nouvelle approche des ressources naturelles*, De Boeck, 2010, 300 p. ; ELINOR Ostrom et ELOI Laurent, « Pardelà les marchés et les États. La gouvernance polycentrique des systèmes économiques complexes », *Revue de l'Observatoire français des conjonctures économiques*, n° 120, 2012, pp. 13-72, ; BRONDIZIO Eduardo S., OSTROM Elinor et YOUNG Oran R, « Connectivité et gouvernance des systèmes socio-écologiques multilatéraux : le rôle du capital social », *Management & Avenir*, n° 67, juillet 2013, pp. 108-140. Pour l'application en criminologie, voir DUPONT Benoît, 2016, op-cit.

proactives, conformes aux meilleures pratiques et obligeant les développeurs de matériel et de logiciels à promouvoir la résilience de leurs produits. Troisièmement, les recommandations d'organisations techniques telles que l'IETF devraient être rendues contraignantes et applicables par les nations lorsqu'elles seront adoptées comme les meilleures pratiques de l'industrie pour contribuer à la protection contre les passagers clandestins. Quatrièmement, les gouvernements et les ONG devraient non seulement continuer à participer aux efforts des États-Unis pour promouvoir la cybersécurité mondiale et affiner la gouvernance de l'Internet par plusieurs parties prenantes, mais également à créer des forums plus restreints pour permettre des progrès plus rapides sur des questions fondamentales d'intérêt commun. Enfin, des campagnes de formation et des partenariats public-privé plus solides devraient être entrepris pour partager les informations et éduquer les parties prenantes à tous les niveaux sur la nature et l'ampleur de la cybermenace. »⁹⁴⁶

Sans s'attarder sur le caractère pro-États-Unis de ces développements, malgré une analyse poussée l'auteur semble exclure une grande partie de l'évolution normative qu'il appelle et qui se déroule déjà sous ses yeux. Pour rappel, la période 2009 – 2014, représente une grande vague de conventions régionales ainsi que de réforme du concept stratégique de l'OTAN ainsi que de la première version du Manuel de Tallinn dont les travaux d'élaboration étaient connus.

2 – La société civile globale et prise en compte des réseaux transnationaux.

En parallèle de cette question de la gouvernance, émerge une question proche qui vient nourrir le débat sur la diversité des acteurs. Il s'agit de l'autonomie de la société civile et en particulier de l'idée de société civile globale qui se manifestera par des groupes transnationaux existant et fonctionnant au-delà des frontières internationales et indépendants de l'autorité des États⁹⁴⁷. Toute la question est ici de savoir si la technologie permet de faire rentrer en concurrence ce type d'acteurs émergents avec les autres acteurs des Relations Internationales, en particulier les États.

⁹⁴⁶ SHACKELFORD Scott J., 2013 op-cit. p. 1364.

⁹⁴⁷ LIPSCHUTZ Ronnie D. « Reconstructing World Politics – the Emergence of Global Civil Society, » *Millennium* vol. 21, n°3, 1992, pp. 389-420. Voir également, BROWN Chris. « Cosmopolitanism, World Citizenship and Global Civil Society. » *Critical Review of International Social and Political Philosophy*, vol. 3, no. 1, 2000, pp. 7–26. Ainsi que ARCHIBUGI Danielle, et al. *Re-Imagining Political Community: Studies in Cosmopolitan Democracy*. Stanford University Press., 1998, 357 p.

Nous avons déjà cité l'exemple des entrepreneurs transgouvernementaux d'Abraham Newman dont le concept pourrait s'en rapprocher. Néanmoins, il ne mobilise pas le concept de société civile globale. En effet, le concept se retrouve plutôt dans la littérature d'inspiration constructiviste. Sur cette question particulière, nous retrouvons globalement diverses postures critiques par rapport aux premiers ouvrages enthousiastes sur la société de l'information⁹⁴⁸.

Parmi les travaux du début des années 2000, ceux de Edward Comor se concentrent sur le rôle de la communication dans les théories consacrées à la société civile globale⁹⁴⁹. Les théories sont riches en termes d'assertions sur le rapport de la communication avec la conscience, l'identité et les conceptions de la réalité. C'est principalement ce rapport que l'auteur va critiquer. Cette critique est construite pour une première partie autour de la remise en question du lien immédiat entre information et connaissance. Plus d'information, ne signifie pas forcément une meilleure connaissance disponible et un meilleur emploi de celle-ci. Cela aboutit au fait que l'accroissement des communications transnationales ne stimule pas nécessairement le type de communauté mondiale progressiste anticipée.

Il y aurait ainsi une surestimation de l'impact identitaire de la communication. Celle-ci n'interviendrait qu'indirectement au travers de son influence sur les modes de vie. Lesquels modes de vie viennent dès lors remettre en cause, le caractère « global » de la société civile anticipée, étant donnée la pluralité et la profonde inégalité qui subsiste entre les populations. L'auteur en déduit que la théorie de la société civile globale méconnait les contextes historiques des relations entre la société civile et l'État. Ce qui pose par ailleurs des questions sur la compatibilité de la société civile globale avec l'économie politique. En particulier, lorsque celle-ci concerne le développement international des moyens de communications.

Dès lors, un regard optimiste sur la théorie de la société globale apparaît comme prématuré aux yeux de l'auteur. Sur l'identité à proprement parler, l'auteur souligne que l'utilisation des nouvelles technologies par les acteurs politiques peut servir à faciliter l'échange de données et la coordination spatiale des activités, mais peut aussi paradoxalement affaiblir les capacités réflexives collectives, suscitant une mobilisation rapide mais laissant peu temps pour

⁹⁴⁸ Voir notamment l'ouvrage CASTELLS Manuel, 1996, op-cit.

⁹⁴⁹ COMOR Edward, « The Role of Communication in Global Civil Society: Forces, Processes, Prospects, » *International Studies Quarterly*, vol 45 n°3, 2001, pp 389-408

la réflexion critique. Dès lors, l'influence directe d'Internet sur l'identité est loin d'être démontrable pour l'auteur même en considérant l'objet du mode de vie.

Opérant des critiques similaires, Ronald Deibert écrit au sujet de la société civile globale en 2003⁹⁵⁰. Il souligne que, pour la plus grande partie d'entre-elles, les théories de la société civile globale sont fondées l'hypothèse de la rapidité et de la portée mondiale des nouvelles technologies de l'information et de la manière dont ces propriétés ont entamé d'importants changements dans l'architecture de l'ordre mondial organisé autour de l'État vers une société construite sur le réseau⁹⁵¹. Il inclut dans sa comparaison théories la société civile globale, mais aussi le citoyen du monde et la démocratie cosmopolite. Il ajoute néanmoins que quelle que soit la pertinence de cette idée, la recherche de régulation et de control d'Internet de la part des secteurs du commerce et de la sécurité affecte l'activité des « réseaux civiques globaux »⁹⁵² et les perspectives d'obtenir un environnement de communication global et ouvert.

Sa démonstration poursuit ici deux objectifs : d'une part, mettre en avant la sécurité et les pressions pesant sur Internet ; d'autres part inciter les Théories des Relations Internationales à prendre en compte ce que l'auteur désigne comme les « facteurs matériels » (les moyens de communication). Le média n'est pas un dispositif creux permettant la communication mais fournit également des opportunités et des contraintes du seul fait de son emploi⁹⁵³.

« Les médias facilitent, modèlent et limitent certes les possibilités de la communication humaine, mais il est important de garder à l'esprit que les médias eux-mêmes évoluent également dans le temps. »⁹⁵⁴

Le concept de médias de l'auteur intègre ainsi le principe du biais technologique qui veut qu'une technologie de communication modifie l'environnement dans lequel la

⁹⁵⁰ DEIBERT Ronald J., 2003 op-cit.

⁹⁵¹ Ibid. p. 502.

⁹⁵² Selon l'auteur, un réseau civique est un ensemble de forces sociales combinées autour des questions d'accès, de confidentialité et de diversité dans les principes, règles et technologies qui configurent les communications globales.

⁹⁵³ Ibid. p 503.

⁹⁵⁴ Ibid. p. 505 (notre traduction)

communication s'opère⁹⁵⁵. De manière générale, il reproche aux auteurs de la société civile globale de ne pas avoir reconnu le rôle constitutif de la technologie dans les phénomènes qu'ils analysent.

« L'anti-matérialisme du travail constructiviste récent, qui constitue la toile de fond principale de la plupart des travaux sur les réseaux civiques, peut expliquer le mépris des technologies de la communication. »⁹⁵⁶

Les pressions sont de trois natures : les censures commerciale et étatique, la surveillance électronique et la militarisation. Elles s'opposent à l'ouverture du média. L'analyse de ces menaces amène l'auteur à s'interroger sur les rapports de la sécurité transnationale de l'information avec la société civile globale. De manière générale, les théories de la mondialisation, de la société civile mondiale et des réseaux transnationaux ont suivi une trajectoire continue de communications de plus en plus ouvertes et distribuées.

Cependant, Ronald Deibert souligne un double manque de communication général entre les réseaux civiques (ONG notamment) et les spécialistes en informatique. Pourtant bien, que les principes n'aient jamais été officiellement codifiés, une constellation de valeurs rassemble ces groupes pour aider à définir un programme commun. Programme commun, que l'auteur appelle de ses vœux. Les contraintes matérielles et le code informatique pourraient à terme constituer les mécanismes les plus importants pour garantir qu'une infrastructure de communication appuie, au lieu de nuire, le projet en cours de gouvernance démocratique globale⁹⁵⁷.

Des auteurs de la seconde moitié des années 2000 se positionnent également de façon critique sur la société civile globale. Par exemple, Emma Murphy étudie la possibilité d'une sphère publique du monde arabe créée dans le cadre d'une connectivité globale⁹⁵⁸. Cette sphère publique arabe comprendrait plusieurs publics et semble émerger du fait de l'intégration des

⁹⁵⁵ Il s'inspire ici de la théorie sociale de la communication. Il reprend en particulier les travaux sur les médias de Harold Innis. INNIS, Harold A. (1951), *The Bias of Communication*, University of Toronto Press, 1977, 226 p.

⁹⁵⁶ DEIBERT Ronald J., 2003 op-cit, p. 522.

⁹⁵⁷ Ibid. p. 530.

⁹⁵⁸ MURPHY Emma C. « Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere. » *International Studies Quarterly*, vol. 53, no. 4, 2009, pp. 1131–1153

nouvelles technologies de l'information et des communications. La sphère publique arabe ainsi créée permet de contester les structures de pouvoir locales et mondiales⁹⁵⁹. Toutefois, cette sphère existe à la périphérie des réseaux mondiaux de l'information. Cela entraîne une dégradation de son attractivité et de la contestation qu'elle permet. Cela est principalement du au fait qu'Internet est principalement dominé politique et idéologiquement par des impératifs commerciaux. On retrouve donc une critique du contrôle des technologies de l'information qui va dans le même sens que la critique de Ronald Deibert sur l'impact négatif du commerce sur le développement politique d'Internet⁹⁶⁰.

3 – Les technologies de l'information et sécurité dans le développement.

Riche de nombreuses approches et de disciplines académiques, l'ensemble des théories du développement renvoie à la différence qui existe entre les États et aux moyens de réduire celle-ci⁹⁶¹. Il est intéressant de se concentrer ici sur certains objets et la manière dont ils nous renseignent sur la place des technologies de l'information dans ces travaux.

L'un des concepts les plus intéressants à la base de réflexion en termes de développement sur les technologies est celui de « fracture digitale » ou de « fracture numérique » que nous avons déjà évoqué⁹⁶². Cette fracture est utilisée pour mettre en lumière les inégalités dans l'accès à un ordinateur ou à Internet, dans l'usages des outils numériques comme dans l'usage des informations qui en sont issus. Sous un prisme International, cette notion permet de traduire les différences de développement de l'informatique entre les États mais aussi de mesurer le caractère plus ou moins fermés de ces outils dans les États en

⁹⁵⁹ « Bien que cette nouvelle sphère publique ne soit pas totalement inclusive et qu'elles tendent à filtrer les diversités culturelles [...] » Ibid. p. 1148.

⁹⁶⁰ Sur ce point, on peut rapprocher l'étude d'Internet dans le contexte arabe de celles conduites sur la télévision. SAKR Naomi. *Satellite Realms Transnational Television, Globalization and the Middle East*. I.B. Tauris, 2001, 280 p. ; SAKR Naomi. *Arab Television Today*. I.B.Tauris, 2007, 256 p.

⁹⁶¹ SCHUURMAN Frans J. « Paradigms Lost, Paradigms Regained? Development Studies in the Twenty-First Century. » *Third World Quarterly*, vol. 21, no. 1, 2000, pp. 7–20.

⁹⁶² Cf. chapitre 1.

question⁹⁶³. La fracture numérique n'est pas forcément limitée à une répartition territoriale⁹⁶⁴. Les causes de la fracture numérique mondiale varient selon les recherches. Dans les travaux scientifiques, elle procède soit des écarts de revenus ou de richesse⁹⁶⁵, soit d'un ensemble complexe de questions économiques, politiques et socioculturelles⁹⁶⁶, soit du niveau d'intégration dans l'activité de la société internationale⁹⁶⁷. Les auteurs ne sont pas vraiment d'accord sur les causes de la fracture digitale ou les moyens d'y remédier.

Prenant l'exemple des États africains, Chris Alden évoque en 2003 un certain nombre de barrières qui forment autant d'obstacles au développement par le biais des technologies de l'information. Il considère notamment que l'approche de la technologie comme remède miracle ne tient pas compte des éléments essentiels de la situation des Africains⁹⁶⁸. Au-delà des barrières économiques, l'Afrique doit tout d'abord faire face à des difficultés d'ordre technique. La connectivité Internet reste à des niveaux très bas par rapport au reste du globe. Les téléphones portables n'étaient pas non plus suffisamment bien répandus. Les infrastructures de communication étaient dans un état particulièrement dégradé du fait de vol de cuivre dans les câbles téléphoniques. Le réseau électrique dans plusieurs États n'est pas non plus suffisamment solide pour assurer une connexion stable et peut endommager une partie des équipements. Sur un plan un peu différent, les ressources humaines ne sont pas disponibles pour permettre le développement par les technologies de l'information. Et enfin, viennent s'ajouter des obstacles politiques⁹⁶⁹.

⁹⁶³ Cela nous ramène à la censure et aux questions posées dans le cadre des recherches sur la société civile globale et de la gouvernance.

⁹⁶⁴ Nous pouvons ici citer l'étude qualitative de Ruth Abbey et Sarah Hyde qui étudient l'effet de l'âge des populations sur la fracture numérique. ABBEY Ruth et HYDE, Sarah, « No country for older people? Age and the digital divide », *Journal of Information, Communication and Ethics in Society*, Vol. 7 No. 4, 2009, pp. 225-242.

⁹⁶⁵ CHINN Menzie D. et FAIRLIE Robert W, « The Determinants of the Global Digital Divide: A Cross-Country Analysis of Computer and Internet Penetration. », *Oxford Economic Papers*, vol. 59 n°1, 2007, pp. 16–44. ; KIM Chon-Kyun « A Cross-National Analysis of Global E-Government.», *Public Organization Review*, vol. 7 n°4, 2007, pp:317–329.

⁹⁶⁶ GUILLEN Mauro F., et SUAREZ Sandra L. « Explaining the global digital divide: Economic, political and sociological drivers of cross-national Internet use. » *Social forces* vol. 84 n°2, 2005, pp. 681-708.

⁹⁶⁷ DRORI Gili S., et JANG Yong Suk « The global digital divide: A sociological assessment of trends and causes. » *Social Science Computer Review* vol. 21 n° 2, 2003, pp. 144-161.

⁹⁶⁸ ALDEN Chris. « Let them eat cyberspace: Africa, the G8 and the digital divide. » *Millennium* vol. 32, n°3, 2003 : pp. 457-476.

⁹⁶⁹ Ibid. pp 469 – 472.

Un autre ensemble de travaux intéressant à la fois les technologies de l'information et le développement peut se trouver dans l'application de l'information aux États compris comme des puissances émergentes. Cela renvoie aux débats sur le concept de puissance. Il existe une grande pluralité des modèles de puissance applicables aux États « émergents » qui se caractérisent selon Delphine Deschaux-Dutard par trois critères : des postures de résistance ou de propositions normatives alternatives, conduites par un individualisme pragmatique sur les plans économique et diplomatique, visant à combler les importants déséquilibres auxquels ces puissances sont confrontées⁹⁷⁰.

Dans ce contexte, les technologies de l'information peuvent être mobilisés en tant qu'éléments d'une stratégie visant à produire cette émergence Toutefois, appliquée à la question de l'émergence, la sécurité ne laisse pas nécessairement beaucoup de place aux technologies de l'information en tant que telle. L'émergence de puissances politiques n'est pas un processus historique uniforme répondant aux mêmes lois. Et pourtant, dans une vision classique de cette problématique une majorité des études se focalisent sur des questions d'armement ou de désarmement. Il en résulte une vision contingente de la technologie. Celle-ci est une des variables qui produira la différence entre deux États dans un domaine d'application particulier. Les technologies de l'information ne sont qu'une modalité supplémentaire du potentiel technologique et scientifique d'un État et n'apporteraient ainsi pas de renouveau sur le terrain⁹⁷¹.

⁹⁷⁰ Avec la nuance que le qualificatif d'émergent conduit à la construction d'un outil de reconnaissance inégalitaire qui ne favorise pas tant un rééquilibrage des rapports de force au sein des Relations Internationales mais intègre lesdits États dans un rapport de subordination. DESCHAUX-DUTARD Delphine et LAVOREL Sabine (dir.), *Puissances émergentes et sécurité internationale : une nouvelle donne ? Une perspective pluridisciplinaire sur la puissance et l'émergence sur la scène internationale*, Bruxelles, Peter Lang, 2017, 312 p. Pour un exemple consacré à l'Inde, MITRA Raja. « Emerging state-level ICT development strategies » *Information and communication technology in development: Cases from India*, 2000, pp.195-205.

⁹⁷¹ Pour aller plus loin, il faut quitter le terrain des Relations Internationales pour aller vers la Géopolitique. Voir notamment HANNES Ebert et MAURER Tim, « Revendications sur le cyberspace et puissances émergentes », *Hérodote*, vol. 152-153, no. 1, 2014, pp. 276-295.

4 – L’impact de la technologie sur les régimes politiques : le cas des régimes autoritaires.

Un autre domaine d’étude est l’analyse de l’impact des technologies de l’information sur les régimes politiques, et autoritaires en particulier⁹⁷². Le postulat de départ est ici que les technologies agissent en faveur de la démocratie et contre le caractère autoritaire des régimes politiques qui utilisent les technologies. Ce postulat a servi de base tenter d’appliquer la théorie du « dilemme du dictateur » aux technologies de l’information. La théorie du dilemme du dictateur s’inspire du dilemme de la croissance qui suppose l’acceptation d’un risque pour obtenir de la croissance économique. Pour bénéficier des avantages potentiels et supposés offerts par les technologies de l’information, les autorités des régimes autoritaires doivent accepter les risques politiques qu’induisent ces technologies. Pour que les nouvelles technologies de télécommunication créent ce dilemme pour les dictateurs, ces technologies doivent être différentes des technologies précédentes, souvent considérées comme des outils permettant aux dirigeants totalitaires de maintenir une « emprise féroce sur la société »⁹⁷³.

Une fois ce principe énoncé, il nous faut opérer un détour et se demander les raisons pour lesquelles un État opte pour une technologie en particulier. Comme nous l’avons vu avec le concept de fracture numérique, les différences dans l’adoption de la technologie séparent les régions et les pays les plus performants sur le plan économique du reste. De plus l’adoption de la technologie est profondément liée aux questions de libertés politiques. Les technologies basées sur la connaissance peuvent favoriser les libertés et leur adoption repose en partie sur les libertés existantes⁹⁷⁴.

Dans leur article de 2006⁹⁷⁵, afin de proposer une théorie de l’adoption des technologies de l’information, Javier Corrales et Frank Westhoff établissent une comparaison de l’adoption

⁹⁷² CORRALES, Javier, et WESTHOFF Frank. « Information technology adoption and political regimes. » *International Studies Quarterly* vol. 50. n°4, 2006, pp. 911-933.

⁹⁷³ KEDZIE Christopher R., *Communication and Democracy: Coincident Revolutions and the Emergent Dictators*. Santa Monica, RAND Corporation, 1997, 120 p.

⁹⁷⁴ NORTH, Douglass C. *Institutions, Institutional Change and Economic Performance*. Cambridge University Press, 1990, 152 p.

⁹⁷⁵ CORRALES, Javier, et WESTHOFF Frank, 2006, op-cit.

de deux technologies particulières : la télévision et Internet. Il y a classiquement deux écoles pour comprendre l'adoption d'une technologie : soit celle qui analyse la réception des caractéristiques techniques de la technologie elle-même⁹⁷⁶, soit celle qui se concentre sur les caractéristiques des acteurs qui l'adoptent (qui se divise ensuite entre approches microsociologiques et macrosociologiques) ⁹⁷⁷.

Après analyse, il apparaît selon eux que la fracture numérique entre les États est le résultat des variations des niveaux de connectivité externe, du développement socio-économique et des politiques des États. Parmi les politiques des États, les facteurs les plus importants semblent être la mesure dans laquelle les États accordent des libertés politiques et poursuivent des politiques de croissance axées sur le marché. Le fait d'avoir moins de libertés est un obstacle pour adopter les technologies de l'information. Les États autoritaires sont souvent contre Internet et adoptent des politiques restrictives. A cela s'ajoute les revenus économiques des habitants.

« Les régimes autoritaires favorisent les technologies de l'information dont ils peuvent contrôler le contenu. Alors que l'architecture d'Internet continue d'évoluer, donnant aux États davantage de capacité de contrôle du contenu, la propension des régimes autoritaires à restreindre l'utilisation d'Internet diminue. En outre, les États autoritaires à revenu élevé, avec une forte croissance et une forte économie de marché encouragent Internet à tirer parti de son efficacité en matière d'économie de coûts, plus que d'autres dictatures. »⁹⁷⁸

Les auteurs affirment ici que leur étude ne permet pas de souscrire à l'idée d'une mise à mal des régimes autoritaires par le biais de l'information. Internet, comme les facteurs qui conduisent à son utilisation accrue, ont transformé les pratiques autoritaires des régimes en question. Elles ne les ont pas supprimées.

⁹⁷⁶ Voir la synthèse sur les approches de la diffusion de l'innovation : ROGERS, Everett M. (1962) *Diffusion of Innovations*. Free Press, 1995, 512 p.

⁹⁷⁷ MACKAY, Hughie, and GILLESPIE Gareth. « Extending the Social Shaping of Technology Approach: Ideology and Appropriation. » *Social Studies of Science*, vol. 22, no. 4, Nov. 1992, pp. 685–716,

⁹⁷⁸ CORRALES, Javier, et WESTHOFF Frank, 2006, op-cit. p.930. (Notre traduction).

5 – Le concept de Cyberpower et les Relations Internationales

Le terme de *Cyberpower* a émergé dans la littérature commerciale des années 90. L'une des premières importations de ce terme dans les sciences humaines a lieu en 1999 avec l'ouvrage de Tim Jordan⁹⁷⁹. Il y présente le terme « cyberpower » comme un moyen d'étudier le cyberespace comme domaine de l'individu. Ce terme décrit la forme du pouvoir qui structure Internet et le cyberespace. Ce pouvoir repose sur la mise en relation de trois composantes : les individus (les possessions individuelles dans un environnement fait d'avatars et de hiérarchie virtuelles), la société (la domination d'une élite virtuelle formée à partir du réseau d'information) et l'imaginaire (l'utopie et la dystopie de l'univers virtuel où le pouvoir apparaît comme le constituant de l'ordre social).

Le deuxième ouvrage intéressant a été publié en 2009. Il s'agit de l'ouvrage collectif dirigé par Franklin Kramer, Stuart Starr et Larry Wentz, *Cyberpower and National Security*⁹⁸⁰. Il contient deux chapitres tentant une conceptualisation du *cyberpower*, respectivement écrits par Daniel Kuehl⁹⁸¹ et Stuart Starr⁹⁸². Le concept y apparaît par analogie aux autres domaines militaires et en référence à la pensée stratégique. Puisque le cyberespace est un « environnement », le *cyberpower* décrit la capacité à agir au mieux dans cet environnement. Il s'agit donc de la capacité d'utiliser le cyberespace pour créer des avantages et influencer les événements dans tous les environnements opérationnels et à travers les instruments de pouvoir⁹⁸³. Cette définition souligne un effet de synergie avec les autres formes et instruments de pouvoir, qu'elle intègre directement à son modèle.

Il faut attendre l'année 2010 pour que le terme *cyberpower* devienne un concept destiné à expliquer des phénomènes en Relations Internationales avec la publication de l'étude de

⁹⁷⁹ JORDAN Tim. *Cyberpower: the Culture and Politics of Cyberspace and the Internet*, Londres, Routledge, 1999, 248 p.

⁹⁸⁰ KRAMER, Franklin D., et al. (dir) *Cyberpower and National Security*. Center for Technology and National Security Policy, 2009, 664 p.

⁹⁸¹ KUEHL, Daniel T. « From Cyberspace to Cyberpower: Defining the Problem » In. KRAMER, Franklin D., et al. (dir) *Cyberpower and National Security*. Center for Technology and National Security Policy, 2009, pp. 24–42.

⁹⁸² STARR, Stuart H., « Toward a Preliminary Theory of Cyberpower. » In. KRAMER Franklin D., et al. (dir) *Cyberpower and National Security*. Center for Technology and National Security Policy, 2009, pp. 43–88.

⁹⁸³ KUEHL, Daniel T. , 2009, op-cit p. 38.

Joseph Nye intitulée *Cyber power*⁹⁸⁴. Défini comme un comportement, il suppose d'obtenir des résultats préférentiels en utilisant les ressources informationnelles du cyberdomaine. Ce cyberdomaine est composé des ordinateurs, d'Internet, des intranets, des téléphones portables et les communications spatiales. Joseph Nye reprend ici la définition de Daniel Khuel qu'il enrichit⁹⁸⁵. Là où l'approche de Nye va se distinguer c'est dans la combinaison du cyberpower avec les concepts de hard power et de soft power. Joseph Nye construit une typologie des cibles qui regroupe la distinction entre instruments physiques et d'informations, la distinction entre *intra cyberspace power* et *extra cyberspace power* selon que l'action dans le cyberespace a des effets en dehors du cyberespace ou pas. *Soft power* et *Hard power* varient en contenu en fonction de cette typologie.

Ainsi du point de vue des instruments d'information, dans le dimension interne au cyberespace, le *Hard power* représentera la capacité à réaliser des attaques par déni de service tandis que le *Soft power* représente la capacité à faire adopter des normes et des standards. Si on sort du cyberespace, le *Hard power* représente l'attaque de système de contrôle et d'acquisition de données (SCADA). Le *Soft power* représente la capacité à réaliser une campagne de communiquer afin d'influencer l'opinion publique.

Du point de vue des instruments physiques, *Hard power* et *Soft power* représenteront le contrôle de l'acteur soit sur des compagnies spécialisées dans le secteur des technologies, soit son action en faveur d'organisations militantes pour les droits de l'homme. A l'extérieur du cyberespace, le *Hard power* signifie la destruction des infrastructures physiques des réseaux d'information. Le *Soft power* représente la capacité à organiser des manifestations en vue de dénoncer les cyberagresseurs.

⁹⁸⁴ NYE Joseph S., *Cyber power*, Harvard Kennedy School, Belfer Center for Science and International Affairs, mai 2010, 30 p. Cela vient compléter une série de travaux antérieurs sur la notion de puissance où Nye comptaillise sept éléments pour construire la puissance d'un État : les ressources de base (territoire et population), la capacité d'action militaire, la capacité économique de production, le potentiel scientifique et technologique, la cohésion nationale, le rayonnement culturel et l'influence de l'État dans les institutions internationales. Voir notamment NYE Joseph S., « The Changing Nature of World Power », *Political Science Quarterly*, vol. 105, n° 2, été 1990, pp. 177-192.

⁹⁸⁵ Ibid. p 4.

Ce pouvoir peut principalement être utilisé pour manipuler un autre acteur de trois manières différentes : l'incitation à un comportement, l'exclusion d'un comportement, et enfin la définition des préférences comportementales d'autrui.

« Le premier aspect du pouvoir est la capacité d'un acteur à faire en sorte que les autres agissent contrairement à leurs préférences ou stratégies initiales. [...] Le deuxième aspect du pouvoir est la définition de l'agenda ou l'encadrement dans lequel un acteur exclut le choix d'un autre en excluant ses stratégies. [...] Le troisième aspect du pouvoir implique qu'un acteur modifie ses préférences initiales de sorte que certaines stratégies ne soient même pas prises en compte. »⁹⁸⁶

Ce type d'actions n'est pas forcément nouveau et ne semble pas justifier la création d'un concept. Ce qui est particulièrement nouveau réside dans les moyens technologiques de ces actions permettant à des acteurs de moindre importance d'avoir recours à ces actions grâce à un faible coût d'entrée, à l'anonymat et plus généralement grâce au caractère asymétrique de la vulnérabilité des acteurs en termes d'information. Du point de vue de Joseph Nye, le cyberspace agit comme un élément de nature à estomper les différences de pouvoir entre les acteurs par la diffusion de celui-ci. Toutefois, il ne s'agit pas pour autant de venir remplacer l'acteur régional. La diffusion du pouvoir n'implique pas une autonomie totale de la part des acteurs. Cette approche de Nye est la plus utilisée pour parler de pouvoir dans les recherches concernant la cybersécurité. Elle n'est pas uniquement mobilisée au sein de l'institutionnalisme néolibéral mais constitue également une base de travail pour les auteurs d'autres courants notamment les auteurs réalistes et constructivistes.

6 – Les normes de cybersécurité par rapport à la description de la menace.

A priori, il faudrait chercher à distinguer la guerre, la criminalité et la sécurité qui sont trois objets différents. Néanmoins leurs comparaisons est utile lorsque l'on chercher à mesurer la cohérence du discours ou les phénomènes d'hypersécurisation. Sans nécessairement pousser la discussion aussi loin dans les théories de la sécurité, c'est tout le sens d'un article publié par Clément Guitton en 2013⁹⁸⁷. L'article produit l'analyse de l'adoption par la France (en 2011), l'Allemagne (en 2005 et en 2011) et le Royaume-Uni (en 2009 et en 2011) de mesures

⁹⁸⁶ Idid. pp 7-8.

⁹⁸⁷ GUITTON Clement. « Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK? » *European Security*, vol. 22, no. 1, 2013, pp. 21–35.

pour sécuriser le cyberespace dans leur propre stratégie de sécurité nationale. L'hypothèse principale de cet article repose sur le postulat d'une qualité injustifiée de la cybermenace en tant que menace à la sécurité nationale. L'article analyse les différents documents de stratégie nationale et compare cette prise en compte de la menace avec les solutions trouvées pour traiter la cybercriminalité. Parmi les principales conclusions de l'article, l'auteur retient que l'adoption de la stratégie de cybersécurité en France, en Allemagne et au Royaume-Uni s'est révélée conforme à leur stratégie de sécurité nationale, mais les ressources déployées n'ont pas été adaptées au niveau associé à la menace. La faible concentration des stratégies sur la lutte contre la cybercriminalité visant à réduire l'insécurité ne semble pas cohérente avec les objectifs annoncés à l'époque.

Pour avoir une politique efficace de nature à impacter durablement la cybermenace, Clément Guitton préconise deux changements de paradigme : d'une part, un élargissement de la notion de cyberattaquant ; d'autre part, une production de produits informatiques sécurisés. Les organismes chargés de l'application de la loi doivent avoir les moyens de renforcer leur pouvoir d'action pour lutter contre la cybercriminalité. Tandis que les entreprises doivent être contraintes et/ou incitées à ne pas mettre sur le marché de produit dangereux ou non-sécurisés⁹⁸⁸. Malgré quelques labels, il n'y a que peu d'incitation à rechercher cette sécurité dans la production de logiciels ou de matériels. De plus, les « producteurs » ont une certaine tendance à transférer la responsabilité du risque à l'utilisateur final du produit.

« Dans le cas particulier des producteurs de cybersécurité qui insèrent une clause de non-responsabilité dans leur contrat de licence d'utilisateur final, le contrat est considéré comme un contrat au sens de la directive européenne sur le commerce électronique. (Parlement européen et Conseil 2000). La définition des contrats abusifs pour les clauses de déséquilibre, comme dans le cas du transfert de la responsabilité au client à son détriment, s'applique donc dans le cadre de la directive européenne sur les clauses abusives dans les contrats conclus avec les consommateurs (Conseil de l'Europe, 1993). »⁹⁸⁹

La réception de la sécurité de l'information dans le cadre de la littérature autour des enjeux de normes traduit ainsi une image ambivalente de la sécurité partagée entre plusieurs référents et plusieurs théories, regardée positivement ou négativement. Toutefois, certains traits

⁹⁸⁸ Voir également l'article CAELTY Myriam Dunn. « Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. » *Science and Engineering Ethics*, vol. 20, no. 3, 2014, pp. 701–715.

⁹⁸⁹ Ibid. p. 32.

communs se dégage lorsqu'il s'agit d'interroger cette idée par rapport au pouvoir. La première idée est que l'emploi des technologies de l'information crée de nouveaux modes d'échanges qui modifient l'environnement des acteurs. Ces modifications entraînent des phénomènes d'opportunité en faveur des acteurs non-étatiques. L'État demeure le garant de l'ordre social, mais cet ordre social apparaît comme plus permissif. Du point de vue des Relations Internationales, il y a donc plus d'acteurs à prendre en compte quel que soit les théories considérées. Une seconde idée est que cette transformation perçue par l'acteur fait naître un besoin de sécurité chez l'ensemble des acteurs considérés. Les États, les entreprises, les individus recherchent une protection de leurs intérêts.

C – La technologie et la sécurité, source de conflictualité.

Le terrain du conflit est sans doute l'un des terrains les plus riches en termes de publications concernant la sécurité lorsque l'on compare avec les autres domaines. Cela vaut pour les Relations Internationales comme pour les autres disciplines académiques. Il en résulte une production comprenant de nombreux textes⁹⁹⁰ qui concernent à la fois la transformation des organisations de défense et aussi du champ de bataille. La réflexion sur la notion de conflictualité est inspirée des travaux de Daniel Ventre⁹⁹¹. Si nous ne reviendrons pas directement sur le cybercrime, le cyberterrorisme ou le cyberespionnage, la conflictualité permet d'inclure la plupart de ces thématiques et de les élargir au-delà du langage « cyber ». Du point de vue de la sécurité de l'information, le conflit recouvre la propagande, les opérations d'information, les infrastructures critiques, l'espionnage, le terrorisme, la criminalité.

Si on devait résumer les discussions sur la thématique du conflit, deux tendances devraient être prises en compte ici. Les discussions théoriques le cyberspace, son concept, les transformations qu'il induit et plus largement la place des technologies de l'information dans le phénomène. La seconde tendance consiste à aborder la nature de la menace et les moyens potentiels pour y faire face. Ce lieu est aussi le plus susceptible d'être affecté par le phénomène linguistique « cyber ». Sur les exemples retenus, la plupart vont mobiliser des termes « cyber ».

⁹⁹⁰ Relevons une porosité qui survient parfois entre certaines publications académiques et des publications de presses spécialisée. La littérature académique sur le cyber-conflit, contrairement aux tendances réalistes de la littérature de vulgarisation, est principalement constructiviste.

⁹⁹¹ En particulier le concept de cyberconflit. VENTRE Daniel, 2011 op-cit.

Plus encore qu'ailleurs, il y a donc des auteurs qui emploient ou n'emploient pas le langage « cyber », mais cet emploi (ou non emploi) est conceptuellement déterminé et procède d'un choix épistémologique propre à l'auteur.

Dans un premier temps, nous nous focaliserons en particulier sur le statut de la « cyberguerre », la balance *entre l'offensive et la défensive*, avant d'aborder la dissuasion ainsi que la transformation des organisations militaires.

1 – La cyberguerre dans la guerre conventionnelle.

Un premier ensemble de travaux va chercher à distinguer le cyberspace et la cyberguerre dans le phénomène guerrier en général. Sur l'histoire de ce dernier concept, nous avons déjà évoqué la naissance de la cyberguerre sous la plume d'Arquilla et Rondfelt en 1993⁹⁹², ainsi que la critique formulée par l'article et l'ouvrage de Thomas Rid⁹⁹³. Cela renvoie par exemple à toute la littérature que nous avons déjà évoquée sur l'application du concept de « domaine » [militaire] au cyberspace⁹⁹⁴. Du point de vue des Théories des Relations Internationales, au-delà du seul domaine, les auteurs se sont interrogés sur le caractère nouveau ou non de la cyberguerre et de la guerre informationnelle⁹⁹⁵. Dans *The future of power*⁹⁹⁶, Joseph Nye définit la cyberguerre des actions hostiles dans le cyberspace ayant des effets amplifiants ou équivalents à une « violence cinétique majeure ». L'analyse de discours que nous avons opéré nous pousse à retenir une définition plus inclusive. Pourrait être perçue et qualifiée comme cyberguerre entre deux États, la pénétration de réseaux étrangers dans le but de perturber ou de démanteler ces réseaux et de les rendre inutilisables, voire de causer des dommages. Mais la question de l'impact n'a pas nécessairement à être prise en compte. Une autre question induite par l'idée de transformation de la guerre est celle de l'avantage ou du désavantage acquis par le degré de maîtrise du cyberspace. La supériorité du cyberspace dans

⁹⁹² ARQUILLA John et RONFELDT David, 1993, op-cit.

⁹⁹³ RID Thomas, 2011 op-cit. et RID Thomas, 2013, op-cit.

⁹⁹⁴ CARR Jeffrey., 2009, op-cit., VENTRE Daniel, 2011, op-cit.

⁹⁹⁵ ERIKSSON Johan, et GIAMPIERO Giacomello, 2006, op-cit. ; LONSDALE, David J., 1999, op-cit.

⁹⁹⁶ NYE Joseph S., *The future of power*, New York, PublicAffairs, 2011, 320 p. ; voir également la même année, l'article NYE Joseph S., « Nuclear lessons for cyber security? », *Strategic Studies Quarterly*, vol. 5 n°4, 2011, pp. 18–38.

la guerre veut qu'un État acquiert un avantage considérable pour les opérations militaires aux niveaux tactique, organisationnel et stratégique par sa maîtrise du cyberspace⁹⁹⁷.

En 2010, l'ouvrage de Richard Clarke et Robert Knake⁹⁹⁸ met en avant que les cibles les plus probables de la cyberguerre sont de nature civile plutôt que des objectifs militaires. La rapidité avec laquelle des milliers de cibles peuvent être atteintes, presque partout dans le monde, ouvre la perspective de crises extrêmement volatiles. Ils ajoutent que la force qui a empêché la guerre nucléaire, la dissuasion, ne fonctionne pas bien dans la cyberguerre. Ce qui implique qu'il faut s'en détacher.

Dans un ouvrage de 2012⁹⁹⁹, sur lequel nous aurons l'occasion de revenir, Nazli Choucri considère que la cyberguerre peut être catégorisée en trois types généraux ou groupes de conflits, avec des caractéristiques différentes, des degrés d'intensité différents et des manifestations différentes. La typologie fournie est particulièrement générale et permet d'englober la plupart des événements conflictuels internationaux pouvant survenir sur les réseaux. Il y a tout d'abord les conflits concernant la gestion du cyberspace et les fonctionnalités opérationnelles d'Internet. Un deuxième type de cyberconflit implique l'utilisation d'Internet pour obtenir un avantage stratégique et l'utilisation du contrôle politique pour réglementer l'accès cybernétique ou refuser l'accès à un contenu jugé indésirable. Le troisième type de cyberconflit implique des menaces à la sécurité nationale entendue dans un sens large¹⁰⁰⁰.

Afin d'explorer les dynamiques de la cyberconflictualité, Brandon Valeriano et Ryan Maness ont entrepris de collecter des informations sur les cyberinteractions entre États rivaux entre 2001 et 2011 afin de pouvoir définir les caractéristiques du cyberconflit au niveau international¹⁰⁰¹. Les données de leur étude incluent 110 « cyber incidents » et 45 « cyber

⁹⁹⁷ Voir notamment l'ouvrage BRYANT William D., *International Conflict and Cyberspace Superiority: Theory and Practice*, Routledge, 2016, 220 p.

⁹⁹⁸ CLARKE Richard A., et KNAKE Robert K.. *Cyber War: the Next Threat to National Security and What to Do about It*. HarperCollins Publishers, 2010, 320 p.

⁹⁹⁹ CHOUCRI Nazli. *Cyberpolitics in International Relations*. MIT Press, 2012, 320 p.

¹⁰⁰⁰ Ibid. p. 21

¹⁰⁰¹ VALERIANO Brandon, et MANESS Ryan C. « The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11. » *Journal of Peace Research*, vol. 51, no. 3, 2014, pp. 347–360.

litiges » entre États rivaux. Les auteurs constatent ici que l'ampleur et le rythme des litiges entre rivaux ne correspondent pas à la représentation classique des cyberconflits. En effet, seulement 20 des 126 rivaux actifs de leur corpus engagés dans un cyberconflit. Les interactions qui sont découvertes sont limitées en ampleur et en fréquence. En outre, la plupart des conflits en ligne qui sont découverts ont un ton « régional ». Ce qui s'oppose à l'idée de cyberspace sans frontière et de conflit sans limite¹⁰⁰².

Cela nous amène à un point particulier qui est l'idée de prolifération que nous avons déjà évoquée en partie au moment de critiquer le concept de cyberarme. Suite à la parution de l'article de Thomas Rid sur le fait que la cyberguerre n'aurait pas lieu¹⁰⁰³, un débat est né autour de la question de la prolifération. Plus précisément, il s'agissait de déterminer les effets que la prolifération attendue des capacités de cyberguerre aurait sur le caractère et la fréquence de la guerre dans le système international. Il ne s'agit pas ici de parler de déterminer un caractère probable de la cyberguerre en opposition à Rid, mais de travailler sur les effets politiques du développement des moyens de lutte informatique. C'est la question d'un article d'Adam Liff publié en 2012¹⁰⁰⁴. Il s'agit pour l'auteur de désenclaver la notion de cyberguerre qui ne doit pas être traitée de manière isolée. La thèse défendue est que la prolifération de capacités de cyberguerre peut accroître la fréquence des guerres dans le système international dans son ensemble. De plus, les attaques de réseau informatique peuvent être particulièrement opportunes comme déploiement d'un système de force dans des circonstances dans lesquelles une force conventionnelle risquerait des représailles¹⁰⁰⁵. Toutefois, après analyse, Adam Liff conclue que la prolifération des capacités de cyberguerre ne devrait pas accroître de manière

¹⁰⁰² Dans un sens similaire, doublé d'une critique de la littérature, voir également l'article d'Erik Gartzke. GARTZKE Erik, « The Myth of Cyberwar, Bringing War in Cyberspace Back Down to Earth », *International Security*, vol. 38, No. 2, 2013, pp. 41–73.

¹⁰⁰³ RID Thomas, 2011 op-cit.

¹⁰⁰⁴ LIFF Adam P., « Cyberwar: A New “Absolute Weapon”? The Proliferation of Cyberwarfare Capabilities and Interstate War », *Journal of Strategic Studies*, vol. 35 n°3, juin 2012, pp. 401–428. Ce premier article a appelé une réponse de la part de Thimothy Junio.. JUNIO Timothy J. « How Probable is Cyber War?: Bringing IR Theory Back In to the Cyber Conflict Debate, » *The Journal of Strategic Studies*, vol. 36, n°1, février 2013. Réponse ayant elle-même fait l'objet d'un nouvel article : LIFF Adam P., « The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio. » *Journal of Strategic Studies*, vol. 36, no. 1, 2013, pp. 134–138.

¹⁰⁰⁵ L'auteur emploie la notion de *brute force measure*. Nous lui préférions ici le recours au concept de système de force.

significative l'utilité attendue de la guerre. L'effet serait bien là, mais marginal, contrairement aux exagérations dont le discours peut faire l'objet.

« Mon analyse de scénarios [...] m'a amené à conclure que l'effet des capacités de cyberguerre sur la probabilité de guerre entre des acteurs spécifiques dépendra d'autres caractéristiques des acteurs impliqués : spécifiquement, leurs capacités militaires (conventionnelles), technologiques, et leurs capacités organisationnelles. En fonction de ces caractéristiques, ainsi que de la nature même de la transaction, les capacités de la cyberguerre pourraient avoir des effets stabilisateurs ou déstabilisateurs. »¹⁰⁰⁶

Cette conclusion amène à quitter le paradigme d'une coercition envisagée pour maintenir ou changer un *statut quo* politique, au profit d'une conception étendue de celle-ci. Dans cette conception, il faut inclure la dissuasion sur laquelle nous reviendrons. Si on s'en réfère à cette quelques articles, la cyberguerre et le cyberconflit entretiennent un doute au sujet de leur contenu : ils s'inscrivent dans une forme d'hypersécurisation, et leurs rapports à la guerre ne semble pas aussi immédiat que le discours ne le laisse entendre en insistant sur les aspects régaliens.

2 – Cyberespace, un nouvel équilibre entre l'offensive et la défensive.

Pour aller un peu plus loin dans la révision des études sur le conflit, il faut souligner l'existence d'une recherche notamment d'inspiration néoréaliste sur la balance entre attaque et défense dans le cyberespace. C'est une thématique très répandue dans les études sur la cybersécurité toute discipline confondue, notamment en termes de cyberdéfense¹⁰⁰⁷. Cette idée de balance est également reprise de manière plus large dans les études stratégiques. Du point de vue des Relations Internationales, il faut revenir à Erik Gartzke¹⁰⁰⁸. L'approche défendue dans son article de 2013 est relativement intéressante car elle opère une distinction entre ce qui pourrait arriver et ce qui est probable.

¹⁰⁰⁶ LIFF Adam P., 2013, p. 136. (Notre traduction)

¹⁰⁰⁷ Parmi les ouvrages français sur cette thématique dans le domaine des Relations Internationales et plus largement de la Science Politique. Nous pouvons citer : VENTRE Daniel, *Cyberattaque et cyberdéfense*, Paris, Hermès Lavoisier, 2011, 312 p.

¹⁰⁰⁸ En particulier l'article de 2003 : GARTZKE Erik, 2013, op-cit. Ainsi que, GARTZKE Erik et LINDSAY Jon R., « Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. », *Security Studies*, vol. 24, n°2, 2015, pp. 316-348.

Pour l'auteur, dans la cyberguerre, les limitations inhérentes aux possibilités offertes par les moyens informatiques font que la violence de ceux-ci ne devrait pas être considérée à part de la coercition conventionnelle. Une cyberattaque pour fonctionner doit avoir recours au secret à l'instar de toute opération militaire. Mais le besoin de rendre une cybermenace crédible va potentiellement nuire à l'efficacité opérationnelle du fait d'opérer un dévoilement pour convaincre. Par ailleurs, il existe des limitations à ce qu'il est possible de faire sur Internet.

« C'est une chose pour un opposant d'interrompre l'infrastructure, les communications ou la coordination et la planification militaires d'un pays. C'est autre chose de faire en sorte que les dommages causés se traduisent par un changement durable de l'équilibre du pouvoir national ou de sa résolution. Il est peu probable que les cyberattaques se révèlent particulièrement efficaces dans les grandes stratégies, à moins d'imposer un préjudice substantiel et durable à un adversaire. Dans de nombreuses circonstances, peut-être même dans la plupart des cas, cela ne se produira que si la cyberguerre est accompagnée par une force militaire terrestre ou par toute autre action visant à tirer parti de toute incapacité temporaire obtenue via Internet. »¹⁰⁰⁹

Le secret qui entoure le domaine est sans doute le plus grand obstacle épistémologique à l'étude d'un équilibre des puissances. Ne pouvant évaluer la puissance d'un acteur, faute d'une définition efficace de celle-ci ou de l'accès à l'information, il serait trop hasardeux de chercher à définir cet équilibre. Cela n'empêche pas paradoxalement de disposer d'un modèle dominant pour l'attaque et la défense. Le modèle commun à la plupart des publications y compris en dehors des Relations Internationales est que dans le cyberespace l'attaque est plus facile à réaliser et la défense plus difficile à mettre en place. Cette représentation repose sur l'idée erronée que toutes les armes pour attaquer sont disponibles « sur le marché noir » pour un prix modique. Du côté de la défense, elle est jugée plus difficile car le simple fait de voir que l'on est attaqué représente un coût d'entrée important et la défense représente une forme de posture permanente là où l'attaque nécessite uniquement une efficacité ponctuelle. Souvent présenté comme une conclusion, ce modèle semble davantage tenir du postulat ou de l'hypothèse tant les études empiriques manquent à ce sujet.

Joseph Nye voit dans ce modèle d'équilibre la résultante de la structure d'Internet qui est davantage dominée par l'idée de la facilité d'utilisation et la décentralisation de ses

¹⁰⁰⁹ GARTZKE Erik, 2013, op-cit, p. 43.

protocoles, plutôt que par des impératifs de sécurité¹⁰¹⁰. C'est un point où la recherche sur la puissance et Internet vient contredire l'histoire d'Internet qui dénote une fracture entre politique et technique quand il s'agit de sécurité. Internet a été conçu avec une idée de la sécurité : préserver le fonctionnement du réseau téléphonique, en cas de guerre y compris en cas d'attaques nucléaires. Et pour atteindre cette résilience, un réseau décentralisé fonctionne mieux qu'un réseau centralisé. Il serait ainsi plus juste de dire que le curseur de la menace s'est déplacé de l'extérieur du réseau vers l'intérieur de celui-ci. Au sens technique, la question a évolué d'un problème de sécurité environnementale du système à un problème de sûreté de son emploi par les utilisateurs. Ce n'est donc pas un problème d'absence de sécurité dans les mentalités des concepteurs mais simplement que celle-ci n'était pas tournée vers les mêmes objets.

En 2015, Gartzke et Lindsay ont émis une hypothèse qui se rapproche davantage des conclusions de notre recherche¹⁰¹¹. Selon cet article, Internet et le cyberspace donne un avantage à la déception¹⁰¹². Cet avantage est valable en attaque, mais aussi en défense. Dans la mesure où il est possible de tromper un assaillant avec un arsenal varié de pièges. L'un des meilleurs exemples en matière de défense active est leurre (ou pot-de-miel, *honeypot*). C'est une technique qui consiste à attirer des assaillants sur un système leurre afin de les identifier ou de les détruire, en disposant un « appât » destiné à faire croire à l'assaillant qu'il se trouve bien dans le système qu'il souhaitait attaquer. Il existe de nombreux types de ces pièges. Toutefois, il en ressort que l'équilibre entre l'attaque et la défense n'est sans doute pas le meilleur concept pour décrire l'impact du cyberspace sur la guerre et que ce dernier nécessite un concept plus adapté.

3 – Les tentatives de conceptualisation d'une cyberdissuasion.

Avec l'idée d'équilibre des puissances, a émergé la question de la dissuasion (*deterrence*) et son application au cyberspace. La notion de cyberdissuasion apparait en 1994

¹⁰¹⁰ NYE Joseph S., 2010, op-cit. p. 5.

¹⁰¹¹ GARTZKE Erik et LINDSAY Jon R., 2015, op-cit.

¹⁰¹² Les principes, les manœuvres stratégiques et tactiques, et les moyens techniques destinés à tromper l'adversaire et le faire agir dans le sens que l'on souhaite. Selon la publication interalliée sur les procédures AAP-06 Edition 2018 émise par le bureau normalisation de l'OTAN, la déception désigne des « Mesures visant à induire l'ennemi en erreur, grâce à des truquages, des déformations de la réalité, ou des falsifications, en vue de l'inciter à réagir d'une manière préjudiciable à ses propres intérêts ». OTAN, Glossaire, AAP-06, Edition 2018, p.192.

sous la plume de James Der Derian dans un article de vulgarisation¹⁰¹³. En 1996, l'article de Richard Harknett, *Information Warfare & Deterrence* lance une petite mode de la recherche sur la cyberdissuasion qui donnera lieu à plus à des publications sur le sujet de la part d'une vingtaine d'auteurs¹⁰¹⁴. Comme avec l'équilibre défense et attaque, le contexte de la cybersécurité est relativement limitant pour une véritable exploration des moyens de lutte information et de leur capacité de dissuasion. Néanmoins, selon Will Goodman, la connexion entre les contextes de cybersécurité et les capacités conventionnelles rendrait la dissuasion beaucoup plus facile à appréhender que prévue.

« Certains théoriciens soutiennent que c'est assez difficile. Ces sceptiques font valoir des arguments valables ; le domaine du cyberspace pose des défis uniques pour une stratégie de dissuasion efficace. Mais traiter la cyber-dissuasion uniquement en théorie, c'est-à-dire en ignorant le contexte géopolitique dans lequel les cyber-attaques se produisent, exagère involontairement sa difficulté. La cyberdissuasion s'avère plus facile en pratique qu'elle ne semble en théorie, car les cyberattaques sont indissociables du domaine physique, domaine dans lequel la dissuasion a fait ses preuves depuis longtemps. »¹⁰¹⁵

Comme il n'y a pas une seule théorie de la dissuasion, il n'y a pas une seule théorie de la cyberdissuasion. L'ensemble des auteurs ayant travaillé ont formé un ensemble théorique intéressant à étudier mais qui manque d'études de cas pour asseoir ces théories. Afin de dépasser l'impossibilité d'étudier positivement la dissuasion en pratique et le manque de cas à étudier, Will Goodman se propose d'étudier les cas où la cyber-dissuasion « a échoué »¹⁰¹⁶.

Une autre approche intéressante de la cyberdissuasion a été formulée plus récemment en 2018 par Brandon Valeriano et Ryan Maness¹⁰¹⁷. Cette approche veut que la cybersécurité

¹⁰¹³ DER DERIAN James, « Cyber-deterrence » *Wired*, Vol. 2, n°. 9, septembre 1994.

¹⁰¹⁴ HARKNETT Richard, « Information Warfare and Deterrence », *Parameters : US Army War College Quarterly*, vol. 26, n°. 3, 1996, pp. 93-107. Estimation du nombre de publication tirée de GOODMAN Will, « Cyber Deterrence Tougher in Theory than in Practice ? », *Strategic Studies Quarterly*, automne 2010, pp. 102-135.

¹⁰¹⁵ GOODMAN Will, 2010, op-cit. p. 102. En réalité les débats sur la dissuasion conventionnelle sont assez loin d'être tranchés.

¹⁰¹⁶ Ibid. L'auteur prend en compte les cas de l'Estonie en 2007, de la Géorgie en 2008 et trois cas de cyberespionnage en 1998.

¹⁰¹⁷ VALERIANO Brandon, et MANESS Ryan C. « International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain » In. BROWN Chris et ECKERSLEY Robyn (eds.), *The Oxford Handbook of International Political Theory*, Oxford University Press, mars 2018, 16 p. Cette approche globale de la dissuasion s'appuie notamment sur leurs travaux antérieurs. Voir VALERIANO Brandon, et MANESS Ryan C.,

soit dominée par la retenue plutôt que par l'exploitation et l'escalade. Les auteurs critiquent l'applicabilité du concept de dissuasion du fait de propriétés environnementales du cyberespace.

« Les problèmes d'information, de crédibilité et de variance des cyberactions rendent impossible la formulation d'un système de réponses aussi sûr et rigide que les systèmes de dissuasion mis en place pendant la guerre froide. »¹⁰¹⁸

La retenue remplace le principe du cout de la dissuasion par un phénomène d'autolimitation du fait des conséquences d'une action. Dans ce système, la flexibilité et la faible augmentation des coûts rendent la défense possible, et l'idée qui veut que l'offensive soit facile par rapport à la défense dépend principalement du contexte et de l'unité examinée.

« La dissuasion signifie une réponse garantie, de sorte que l'attaquant estime que le coût d'une attaque est trop élevé. En matière de cybersécurité, il y aura probablement une réponse, mais ce n'est pas un moyen garanti, pertinent, ni dans le domaine de l'opération en premier lieu. Elle est nébuleuse, flexible et considérée compte tenu des conséquences des dommages civils dans le cyberespace. »¹⁰¹⁹

4 – Technologies de l'information et transformation des organisations militaires.

La transformation des organisations militaires constitue un champ à part entière que les Relations Internationales partagent avec l'Histoire, la Sociologie militaire, et de nombreuses autres disciplines y compris en dehors des sciences humaines et sociales. L'apport principal des Relations Internationales concernant la sécurité de l'information dans ce champ consiste dans les études sur la guerre réseau-centrée et surtout la révolution des affaires militaires.

Revenue à la mode au lendemain de la Guerre du golfe, la révolution des affaires militaires (RMA) désigne la transformation qualitative dans l'usage de la force par les militaires. Cette notion admet généralement trois conceptions différentes et non-exclusives les unes des autres selon les auteurs. La première conception est la transformation du lien entre l'armée de l'État qui met en avant les déterminants économiques, politiques, culturels de la

2014, op-cit. Ainsi que VALERIANO Brandon, et MANESS Ryan C., *Russia's Coercive Diplomacy : Energy, Cyber, and Maritime Policy as New Sources of Power*, Londres, Palgrave Macmillan, 2015, 250 p.

¹⁰¹⁸ VALERIANO Brandon, et MANESS Ryan C., 2018, p. 7.

¹⁰¹⁹ Ibid. p. 8.

conception de l'emploi des systèmes de forces. La seconde conception repose sur l'idée que l'évolution technologique de l'armement emporte l'évolution du système de force. Et la troisième approche soutient qu'il n'y a pas vraiment de révolution militaire au sens de rupture mais que le système de force évolue en permanence pour s'adapter à l'ensemble des déterminants de son environnement. Du point de vue de la sécurité de l'information, il y a plusieurs contributions intéressantes qui mettent en avant l'intérêt de l'objet dans le cadre de l'étude de ladite révolution.

En 2004, Emily Goldman publie sur les ressources informationnelles dans le cadre de la performance militaire¹⁰²⁰. Le but de cette étude est d'analyser le lien entre la RMA et l'information. Afin de construire la réflexion, l'étude distingue les technologies de l'information, les ressources informationnelles et l'information. L'information étant la donnée, la ressource informationnelle se définit comme « tout dispositif, technologie, corpus de connaissances, personne » ou une combinaison de ces éléments qui est en mesure de « manipuler des informations de telle manière que celles-ci soient clairement différentes après la manipulation »¹⁰²¹. Les technologies de l'information, quant-à-elles, sont principalement des artefacts. Du point de vue des résultats de cette étude, les technologies de l'information semblent principalement utiles aux États qui ont déjà de grandes capacités technologiques à leur disposition. Après 2007, cette tendance s'est inversée au profit d'une préférence pour l'idée d'asymétrie. En 2010, Jacqueline Newmyer a publié un article sur les caractéristiques de la révolution des affaires militaires en Chine¹⁰²². L'article n'est pas focalisé en particulier sur les technologies de l'information. Mais il en ressort, que celles-ci en tant que composante d'une Révolution des Affaires Militaires peuvent permettre à un État d'obtenir des moyens de démontrer sa force à des États plus puissants :

¹⁰²⁰ GOLDMAN Emily O. « Introduction: Information Resources and Military Performance. » *Journal of Strategic Studies*, vol. 27, no. 2, 2004, pp. 195–219.

¹⁰²¹ Ibid. p. 196.

¹⁰²² NEWMYER Jacqueline, « The Revolution in Military Affairs with Chinese Characteristics, » *Journal of Strategic Studies*, vol. 33 n°4, 2010, pp. 483-504.

« Les cyber-intrusions à des fins d'espionnage, de déni de service ou de sabotage ont également la qualité de donner à la Chine un moyen de signaler sa capacité à perturber les opérations civiles et militaires américaines. »¹⁰²³

En dehors de la Révolution des Affaires Militaires, plusieurs grilles de lectures ont été proposées pour décrire le pouvoir facilitateur des technologies de l'information dans la transformation des organisations militaires et en particulier dans le cadre des organisations « en réseau ». Il est possible de penser aux travaux d'Antoine Bousquet sur la guerre chaoplexique¹⁰²⁴. Lequel décrit un système de force organisé en réseau faisant la part belle à des unités décentralisées et très mobiles capables de « *swarming* » (saturer la cible et ses défenses) et d'adapter sa stratégie et sa tactique en temps réel en fonction des réactions de l'adversaire. La cyberdéfense représente ici un stade antérieur au système décrit. L'article présente une typologie composée de quatre stades de la guerre : mécanique (horloge), thermodynamique (moteur), cybernétique (ordinateur) et chaoplexique (réseau). La guerre y évolue à partir du déploiement rigide mécanique jusque dans un système décentralisé où cybernétique devient synonyme de *command and control* et d'automatisation/robotisation du champ de bataille.

Toute la question de ces approches réside finalement dans le fait de savoir si la technologie et en particulier la sécurité de l'information est un catalyseur de la transformation des forces ou la cause d'un processus de transformation.

Conclusions de chapitre.

Ce chapitre avait pour but de faire le lien entre l'emploi d'un langage « cyber » et l'objet de référence que constitue la sécurité de l'information au moyen des Théories des Relations Internationales. Partant des caractéristiques du discours, la théorie de la sécurisation de Nissenbaum et Hansen a permis de traduire le langage en opérateur de conversion de l'information en enjeu de sécurité. Cet opérateur de conversion illustré par les grammaires qu'il mobilisait l'exagération (hypersécurisation), les pratiques quotidiennes et le rôle

¹⁰²³ Ibid. p. 500 (Notre traduction).

¹⁰²⁴ BOUSQUET Antoine, « Chaoplexic Warfare or the Future of Military Organization, », *International Affairs*, vol. 84 n° 5, 2008, pp. 915-929.

particulier des experts (technification) présents dans le discours de la sécurité de l'information et en particulier dans le discours « cyber »¹⁰²⁵. Cela confirmait les analyses issues de la première partie des développements.

Toutefois cet opérateur n'explique pas les causes du phénomène de sécurisation et présentait celui-ci de manière autonome et techniquement valide. Ainsi, il faut élargir le périmètre de la prise en compte du discours pour intégrer les éléments de controverses qui gravitent autour du discours cyber (notamment le manque de précision du langage et le contexte d'émergence particulier à l'emploi de ces termes). Cela revenait à prendre les logiques du discours et à les confronter à l'environnement technique et politique de ses contextes d'emploi. Au-delà de mettre en avant la seule absence d'autonomie du discours qui rendait son sens dépendant dudit contexte, ce chapitre a opéré une mise à distance du terme cyberspace à l'aide de l'évolution des labels de guerre depuis la fin de la deuxième guerre mondiale. Il a également mobilisé l'idée d'intervention des acteurs tiers dans la sécurité de l'information. Pour aller plus loin, ce contexte d'emploi de la sécurité de l'information a été confronté à la réception de celle-ci dans les Théories des Relations Internationales (avec le langage « cyber » ou sans celui-ci). Cela avait pour objectif d'étudier les différentes manières d'aborder les enjeux technologiques de l'information sous le prisme de l'idée de sécurité.

Ces développements ont permis de mettre en avant une certaine forme de déterminisme technologique présent dans les Relations Internationales depuis leurs origines, un impact non négligeable des paradigmes sur l'appréhension de la sécurité de l'information, et enfin, une place importante des récits dans le traitement scientifique de ces enjeux. L'analyse d'un échantillon des thématiques des publications a démontré que la majorité des publications sur la cybersécurité restent axées sur les politiques publiques et la résolution de problèmes avec pour la plupart d'entre elles, un rapport relativement distant à l'empirie. De fait, la technologie apparaît comme une thématique traitée de manière insuffisante dans les Théories des Relations Internationales. En analysant les questions de la gouvernance, de la société civile globale, du développement, des régimes autoritaires de la cyberguerre, de l'équilibre des puissances, de la cyberpuissance, de la dissuasion, de la transformation des organisations militaires ou encore des politiques mises en place par rapport à la description de la menace, l'observateur fait face aux mêmes grands questionnements.

¹⁰²⁵ HANSEN Lene et NISSENBAUM Helen, 2009, op-cit,

Le phénomène de l'information automatisée change-t'il quelque chose du point de vue de la société internationale ? Dans quelle dimension ? Ce changement est-il inéluctable ? Quelles sont les traductions politiques de ce changement éventuel ? Que faire des acteurs qui semblent avoir une capacité à influencer ou agir sur la scène internationale alors que les théories ne l'envisageaient pas forcément ?

Appliqué à chacun des objets décrits, chaque publication opère comme une réponse à ces questions fondamentales. Articulée autour des discours utopique (*utopian*), réglementaire (*regulatory*) et réaliste (*realist*)¹⁰²⁶, la typologie de Mary Manjikian semble être un outil utile pour traduire les grandes oppositions dans les réponses à ces questions, mais ne transcrit pas nécessairement les différences d'approches entre chacun des auteurs sur les objets mentionnés qui appellent le plus souvent des positions hybrides à mi-chemin entre au moins deux des modèles présentés.

En combinant les apports de l'analyse de discours avec une théorie capable de traduire ce dernier en phénomène politique et une lecture « critique » de la réception de la sécurité de l'information dans les Théories des Relations Internationales, ce chapitre constitue un socle qui alimentera la démarche érotétique et la combinaison pragmatique présentes dans le cinquième et dernier chapitre.

¹⁰²⁶ MANJIKIAN Mary, 2010, op-cit. p. 387.

Chapitre 5 – Au-delà du discours, étudier les Relations Internationales par la sécurité de l’information.

« L'esprit scientifique nous interdit d'avoir une opinion des questions que nous ne savons pas formuler clairement. Avant tout, il faut savoir poser des problèmes. [...] Pour un esprit scientifique, toute connaissance est une réponse à une question. S'il n'y a pas de question, il ne peut y avoir de connaissance scientifique. Rien ne va de soi. Rien n'est donné. Tout est construit. »

Gaston BACHELARD¹⁰²⁷.

Après avoir analysé le cyberespace comme discours de sécurité centré sur l'information, en essayant de prendre en compte son contenu, ses effets, ainsi que son contexte de réception au-delà du seul fait du langage, il nous faut maintenant traiter de l'étude de son objet référent. Nous sommes parvenus à démontrer que l'information est un objet de sécurité. Le langage dérivé cyberespace n'est qu'une manifestation dans un contexte plus large. Ce langage affecte également une partie de la réception de l'objet dans le domaine de la recherche. L'hypersécurisation de l'information rejaillit ainsi sur le travail qui est mené dans la recherche notamment en Relations Internationales.

Partant de notre ligne directrice, ce que nous pouvons déduire et construire du contexte d'emploi de notre discours ne passe non plus par l'analyse, mais au contraire par une forme de distanciation épistémologique. Il s'agit ici d'écartier le phénomène du langage et de s'interroger plus largement sur l'objet de la sécurité de l'information dans toute sa complexité. Ce chapitre est ainsi l'occasion de revenir sur le pragmatisme conduit par les problèmes et de commencer à poser les bases du texte explicatif idéal. Comme nous le soulignons dans le chapitre liminaire, cette approche passe par une forme d'éclectisme qui suppose la combination de théories envisagées comme des outils complémentaires destinés à une compréhension holistique du phénomène. Cette combinaison est conduite par des problèmes spécifiques dont la

¹⁰²⁷ BACHELARD Gaston (1938), *La formation de l'esprit scientifique : contribution à une psychanalyse de la connaissance*, Paris, Vrin, 1993, p. 16.

complémentarité assure la compatibilité et la complémentarité des différentes théories mobilisées.

Ce chapitre sera principalement divisé en deux étapes. La première étape consiste à se demander quelles sont les questions posées aux Relations Internationales par l'objet étudié. Nous avons dégagé quatre grandes questions : le langage, la technologie, l'agentivité et l'information. Celles-ci feront l'objet des développements de notre première section. La deuxième étape consiste à identifier quelles théories répondent au mieux à la plupart de ces questions afin de comprendre les enjeux de l'information dans les Relations Internationales.

Section 1 – Les questions de la sécurité de l'information aux Relations Internationales.

L'examen du phénomène discursif « cyber » et des travaux de recherche sur la sécurité de l'information fait naître un certain nombre de questions. Les questions retenues ici n'étaient pas les seules que ce sujet posait. Nous n'allons pas toutes les détailler, mais revenir sur le processus de sélection des questions.

Afin de sélectionner ces questions, la théorie des contrastes a été mobilisée¹⁰²⁸. Pour rappel, cette théorie veut que toute réponse à une question soit relative au contexte dans lequel celle-ci est posée. Comme nous l'avons dit précédemment, le rôle de la théorie du contraste est de préciser les présupposés qui encadrent la question et de circonscrire la réponse attendue¹⁰²⁹. Le travail autour de la littérature en Relations Internationales, mais aussi sur le discours et l'observation participante dans le milieu français de la recherche, nous ont ainsi mené vers les quatre types de questions qui reflètent les oppositions théoriques sur l'enjeu de la sécurité de l'information. Nous évoquerons les questions par ordre d'importance inversé, de la question ayant le moins d'implications théoriques à la question en ayant le plus.

¹⁰²⁸ CORNUT, 2012, op-cit.

¹⁰²⁹ Pour rappel, cet outil permet de circonscrire ce qui est une bonne explication dans le contexte de la question, ce qui est expliqué (l'espace contrastif), et ce qui n'est pas expliqué (l'extérieur de l'espace contrastif) et donc de construire un cadre de travail pour estimer la pluralité des explications tout en évitant la menace de l'incohérence. Cf. chapitre liminaire.

La première question est celle du langage pour décrire l'objet de recherche. Celui-ci est complètement éclaté et une partie du travail de recherche ne repose que sur des notions. Lorsqu'elle ne repose pas sur des simples poncifs idéologisés. La grande question que nous nous poserons est donc de savoir s'il faut ou ne faut pas utiliser le langage « cyber » à des fins de conceptualisation ? Elle admettra une question corolaire : comment organiser les publications scientifiques qui utilisent ce langage et celles qui le refusent ?

La deuxième question est liée à la première et concerne la technologie. Le langage « cyber » est un processus qui émerge parce qu'il répond à un besoin sociétal. Il faut des mots pour décrire un bouleversement. Il faut encore plus de mots décrire l'invisible et pour réunir différents intérêts autour de problématiques particulières. Le langage « cyber » est l'un des facilitateurs qui permet de traduire les préoccupations autour de la sécurité de l'information. Mais cela recèle un effet pervers. Le cyberspace et les termes dérivés enferment la représentation dans un important déterminisme technique. La question pour les Relations Internationales est donc de savoir comment sortir de ce déterminisme. Il s'agit de l'enjeux de faire que la technologie en tant que processus social soit un objet d'analyse des Relations Internationales.

La troisième question est sans doute l'une des plus difficiles car elle apparaît comme étant constitutive des Relations Internationales. C'est la question de l'agentivité dans un environnement asymétrique. Comment comprendre la faculté d'un acteur à être et agir dans l'information par les Relations Internationales ? Comment comprendre le caractère asymétrique du monde de l'information opposé aux modèles des Relations Internationales ? Cette question représente d'ailleurs une grande part des discussions théoriques entre les auteurs et elle est un enjeu fondamental lors des événements scientifiques. Il apparaît clair qu'un « acteur du cyberspace » au sens sociologique par exemple n'est pas forcément un « acteur des Relations Internationales » dans l'absolu. Mais nous avons retenus que dans certaines circonstances, il pouvait l'être et que cet acteur du cyberspace était l'enjeu des politiques de sécurité de l'information. La situation théorique de l'acteur en ressort particulièrement complexe.

La dernière question que nous avons retenue concerne l'objet référent de la sécurité : l'information. Imaginons que nous savons quels mots choisir, afin d'étudier la technologie et que nous connaissons les acteurs concernés. Encore faudrait-il avoir une vision claire de ce

qu'est l'information. Il y a des théories de la communication et des théories de la décision en Relations Internationales, mais il n'y a pas forcément de théorie de l'information. Savons-nous intégrer l'information au plan ontologique comme l'un de nos objets observables ? Rien n'est moins sûr. Sans voir l'information, comment étudier la sécurité de celle-ci ?

A – La question du langage : l'utilisation du langage « cyber ».

Faut-il se servir du langage « cyber » en tant que source de concepts pour étudier les Relations Internationales ? La question pourrait sembler étrange à ce stade de notre réflexion, considérant que nous avons passé la plus grande partie du manuscrit à étudier cette notion et son sens politique. Et pourtant, la question se pose. Au-delà du discours, le cyberspace doit-il servir de concept aux Relations Internationales ?

La réponse n'est pas simple. D'un côté, c'est un terme utile pour labelliser une recherche et toucher une vaste communauté d'intérêt. D'un autre côté, malgré son fort pouvoir évocateur le terme pêche par son contenu technique. Nous évoquerons d'une part, les faiblesses du langage « cyber », avant d'examiner la question de l'alternative.

1 – Les « faiblesses » du langage « cyber ».

A priori, nous ne devrions pas nous servir du langage « cyber ». En tout cas c'est le conseil d'Andrew Futter en 2018 dans son article qui nous explique pourquoi il faudrait retirer ce dernier « mot à la mode » dans les études de sécurité¹⁰³⁰. Le but de cet article est en effet de soutenir que soutient les études de sécurité et l'élaboration de politiques publiques se portaient mieux sans ce langage. C'est un article intéressant car il reprend la plupart des critiques adressées au vocabulaire.

« La confusion et les malentendus qui entourent l'utilisation du mot « cyber » dans les études de sécurité, stratégiques et militaires et dans l'élaboration des politiques risquent de rendre le concept vide et peut-être même vide de sens lorsque nous parlerons des défis posés aux systèmes et réseaux informatiques. Au mieux, il interdit un débat académique et politique plus fructueux sur la nature, l'étendue et les implications de la dernière ère de l'information ; au pire, cela nous empêche de faire face aux menaces

¹⁰³⁰ FUTTER Andrew, « ‘Cyber’ Semantics: Why We Should Retire the Latest Buzzword in Security Studies. » *Journal of Cyber Policy*, vol. 3, n°2, avril 2018, pp. 201–216.

sérieuses et pressantes qui pèsent sur notre mode de vie. Trop souvent, la même phrase est utilisée pour signifier des choses entièrement différentes, et le plus souvent, le nom de « cyber » semble être utilisé (de manière irresponsable dans certains cas) pour ajouter un sérieux ou une importance accrue sans trop réfléchir à la manière dont cela s'enracine dans notre compréhension plus large du concept. Le résultat est qu'une grande partie du « cyber débat » - en particulier dans le domaine des sciences sociales - a fait l'objet de vives réflexions et de distorsions, les prédictions les plus défavorables étant fondées sur des données relativement peu nombreuses ou des recherches abondantes. »¹⁰³¹

La première des raisons invoquées est qu'au début le cyberspace n'a pas été créé pour ça. Il a commencé dans la vie sans rien avoir à faire avec les études de sécurité, mais il est devenu empêtré dans les débats sur la guerre de l'information et est lentement devenu un terme « fourre-tout »¹⁰³². De notre point de vue, une partie de cet argument est fondé. C'est effectivement les travaux sur la guerre de l'information dans les années 90 qui ont popularisé le terme. Cependant l'autre partie de l'argument méconnait une grande partie de l'histoire de la notion « cyber », puisque celle-ci est profondément liée à l'histoire de la cybernétique, de la conquête spatiale (cyborg), et que la guerre cybernétique existait avant le cyberspace.

Par ailleurs, au risque d'enfoncer une porte ouverte, ce ne serait pas la première fois que les études de sécurité empruntent des concepts directement ou indirectement à d'autres domaines de la connaissance... Cela est plutôt positif en soit et participe du renouvellement de la vie scientifique. De plus, refuser un concept au motif qu'il serait « fourre-tout » ne semble pas recevable sur ce seul argument dans un champ de la connaissance où le concept principal est défini comme étant un « *essentially contested concept* »¹⁰³³.

La deuxième raison est que l'établissement d'une définition convenue du « cyber » et d'un programme de recherche approprié s'est avérée jusqu'à présent impossible. Il est impossible de ne pas être d'accord sur l'aspect de la définition. C'est d'ailleurs une force du cyberspace : un pouvoir évocateur toujours maintenu par une définition insaisissable. Il s'agit d'ailleurs d'un trait commun à tous les concepts polymorphes (démocratie, gouvernance, populisme, totalitarisme, etc.) dont il est difficile de parvenir à une définition consensuelle et qui met à mal le nominalisme qui entoure des termes. Maintenant venons-en à l'idée d'un

¹⁰³¹ Ibid. p. 212. (Notre traduction).

¹⁰³² Ibid. p. 203.

¹⁰³³ GALLIE Walter, 1955, op-cit.

programme de recherche. L'auteur souligne, à raison, la confusion du débat sur le cyberespace et ajoute qu'il est souvent difficile dans les débats de savoir quel type de cadre ou de compréhension est utilisé. C'est une contrainte importante pour qui travaille sur ce type de sujets « à la mode ». Le cyberespace génère beaucoup de travaux et parmi eux, beaucoup n'ont que peu de valeur ajoutée en termes de données ou de démonstration. Néanmoins, cela ne veut pas dire qu'il n'y a pas de travaux de recherche de grande valeur et intéressants pour fonder des programmes de recherche. Cela est très vrai dans le monde anglosaxon. Pour prendre un exemple, aux États-Unis, le projet ECIR (*Explorations in Cyber International Relations*) a été lancé en 2009 (soit environ 9 ans avant la parution de l'article objet de ce commentaire)¹⁰³⁴.

Une troisième raison avancée est que la cybermanace est une utilisée pour désigner des choses très différentes, avec des implications très différentes à la fois en termes d'objectif immédiat et à long terme. La cybermanace désigne tantôt le crime, le hacking, la nuisance, le vandalisme ou encore l'hacktivisme. Il y aurait par ailleurs une différence de nature entre l'attaque qui vise un système informatique et l'attaque qui le système qui dépend de lui. Et enfin, une cybermanace peut viser des informations comme des systèmes informatiques.

« Ainsi, l'idée que nous puissions parler d'une « cybermanace » homogène n'est pas utile, car une gamme aussi large d'activités, de risques et de dynamiques très différentes relève de cette étiquette. La nature, la gravité et les implications de ces menaces varient considérablement et nécessitent donc des formes de réaction très différentes. »¹⁰³⁵

L'approche de la cybermanace que nous avons retenue est ici au contraire une seule et unique chose : il s'agit d'une activité qui vise à comprendre l'intégrité d'un système d'information par l'altération de la disponibilité, de l'intégrité ou de la confidentialité des informations qu'il contient. Le fait que la cybermanace puisse avoir autant de formes et autant d'auteurs potentiels et de motivations différentes vient du fait qu'elle n'est utilisée pour étudier les cyberattaques, ou les cyberincidents. Elle est un élément important de la sécurisation qui

¹⁰³⁴ Crée en 2009, ce projet de recherche interdisciplinaire entre le MIT et l'Université de Harvard a pour objectif d'explorer différentes facettes des relations cyber internationales. Ce programme visait une recherche qui clarifie les menaces et les opportunités dans le cyberespace pour la sécurité nationale, le bien-être et l'influence, et qui fournit des outils analytiques pour comprendre et gérer la transformation et le changement, et enfin attire et éduque une nouvelle génération de chercheurs, d'universitaires et d'analystes. Il s'agissait d'une partie du programme Minerva financée par l'*Office of Naval Research*.

¹⁰³⁵ FUTTER Andrew, 2018, op-cit. p. 207. (Notre traduction)

décrit avant tout de manière pratique une vulnérabilité d'un ou plusieurs acteurs en terme d'information.

Pour l'auteur, le langage « cyber » complexifie la prise de décision politique plutôt que de la simplifier. En effet, ce dernier met l'accent dans le débat sur les plus importantes menaces alors que la plupart des incidents se dérouleraient à la marge et seraient de faible importance. Toutefois, il ne semble pas s'agir ici de la décision politique elle-même que de la compréhension scientifique de cette décision. En témoignent les exemples choisis : la dissuasion remise en cause, l'impossibilité un contrôle des armes ou des accords internationaux significatifs dans le domaine numérique, et enfin la nécessité d'une approche sociétale avec différents niveaux de responsabilité. Cela semble être un faux problème. Aucun des éléments pointés ici n'est dépendant du langage employé. L'information en tant qu'enjeu de sécurité possède les mêmes propriétés que celles qui sont invoquées ici. La sécurité de l'information complexifie la décision politique car elle remet en cause un certain nombre d'acquis. Mais, cela n'est pas (ou pas seulement) dépendant des mots pour le dire.

2 – L’alternative au langage du cyberspace.

L'argument final d'Andrew Futter est qu'il existe déjà dans les études de sécurité des mots pour dire « les défis de l'ère numérique »¹⁰³⁶. L'auteur propose principalement de revenir au concept de la guerre de l'information (*information warfare*) dans laquelle il distinguerait les opérations de type *Computer Network Operations*, elles-mêmes réparties entre les *Computer Network Attack* et les *Computer Network Exploitation*. Autrement dit, les attaques informatiques se limiteraient aux opérations qui ont pour but de causer un dommage. Les autres opérations seraient de l'exploitation. Il faudrait également supprimer la cybersécurité, pour revenir à la sécurité de l'information (protéger l'utilisation de la donnée), la sécurité du réseau (protéger l'accès à la donnée) et la sécurité de l'ordinateur (protéger le système informatique des dommages matériel et logiciel).

Une telle proposition diminue la portée du langage et repose en grande partie sur des concepts erronés qui ne fauilleraient pas le travail et la discussion pluridisciplinaire sur l'objet étude. Par ailleurs, ces appellations entretiennent un paradigme technicien tout en n'étant pas

¹⁰³⁶ Ibid. p. 210.

techniquement correctes. Si on s'intéresse un peu au langage de la sécurité de l'information et notamment au concept de sécurité de l'information proprement dit, il est facile de constater que la typologie proposée méconnait le sens de la sécurité de l'information. La sécurité de l'information est un concept global qui ne se préoccupe pas de la forme de l'information (informatique) pour assurer la protection de celle-ci. Toute les formes de sécurité proposées (réseaux, ordinateurs, informatique) ne sont en réalité que des sous-domaines de ce paradigme global qui prend déjà en compte la disponibilité, l'intégrité, la confidentialité et l'imputabilité de l'information¹⁰³⁷. Le piège ici consiste toujours à vouloir recherche la rigueur d'un concept chez quelque chose qui est une notion, un discours, un label, une métaphore littéraire mais qui n'est pas un concept... Les alternatives au cyberspace sont connues depuis longtemps. En dehors des quelques approches centrées sur les objets (informatique, réseaux, données), il y a quelques termes généraux qui peuvent remplacer le langage « cyber » : l'information, le numérique, le digital...

Faire le choix de s'en remettre au langage « cyber » pour décrire la sécurité de l'information, c'est faire le choix d'un terme au fort pouvoir évocateur qui résiste aux mutations techniques des technologies de l'information tout en intégrant l'ensemble des dimensions de celles-ci. Peu de concurrents peuvent aujourd'hui rivaliser une telle plasticité notionnelle. Néanmoins, c'est également la raison pour laquelle d'aucuns lui préfèrent le mot « numérique » plus propice à représenter le caractère informatisé de leurs préoccupations.

Tout chercheur doit s'interroger sur ce que l'emploi du langage « cyber » apporte à sa recherche. L'observation participante a démontré en cours de thèse que le langage « cyber » élargissait le public de la recherche et favorisait le développement de dynamique interdisciplinaire autour de l'enjeu de la sécurité de l'information. Le langage « cyber » demeure ainsi une prodigieuse source de notions qui favorise la médiation et l'échange entre les différents secteurs professionnels qui forment la communauté épistémique de la sécurité de l'information.

Pour fonctionner, les Relations Internationales et plus largement la Science Politique font appel à des mots qui varient en sens et dont les définitions à elles-seules peuvent nourrir

¹⁰³⁷ Il est possible à ce sujet de renvoyer vers les définitions produites dans le cadre de la norme ISO/CEI 27002 dans sa version de 2013.

des champs entiers de la recherche. L'hypothèse d'un déclin du cyberespace en tant que langage label de la sécurité de l'information est tout à fait probable. Néanmoins, tant que le terme continue de s'inscrire positivement dans les pratiques discursives et normatives des acteurs, il y a lieu de s'interroger sur son sens et sa portée. Par ailleurs, cette notion a une valeur importante en ce qu'elle constitue également l'expression d'un besoin sociétal auxquelles les études de sécurité doivent répondre.

Contrairement à ce que l'auteur énonce sur la légitimité des sciences sociales, il y a une vraie redondance des sciences techniques et des sciences de l'ingénieur sur les projets de recherche qui ont trait à la sécurité de l'information. Le langage pose-t-il vraiment problème ? Qu'un auteur décide d'avoir recours au cyberincident plutôt qu'à l'incident informatique ou à la cyberattaque plutôt qu'à l'attaque informatique est-il vraiment signifiant d'un point de vue scientifique ? Ou alors la distinction n'est-elle qu'artificielle ?

B – La question de la technologie : les apports de la sociologie des sciences et techniques.

Comme dans la plupart des domaines des sciences humaines et sociales, les Relations Internationales se trouvent ainsi écartelées entre la félichisation d'artefacts particuliers et les grandes causes de transformations mobilisent à fin d'expliquer les changements internationaux. La technologie en que processus social ne fait pas partie des objets scientifiques, elle n'est qu'une variable destinée à étudier les objets d'étude légitimes. En adoptant une ontologie critique et discursive pour décrire les trois objets que sont le cyberspace, la sécurité de l'information et la technologie, nous pouvons circonscrire non seulement circonscire la réception du discours de sécurité à l'échelle des relations internationales, mais également déterminer la part qui relève de l'idéal et la part de matérialité.

Afin de sortir du déterminisme technique des Relations Internationales tout en tenant compte des socio-matérialités qui construisent notre objet d'études, il faut considérer les technologies de l'information sous le prisme de la sociologie des techniques et des sciences. Dans le chapitre premier de cette thèse, ont déjà été évoquées la typologie des postures

intellectuelles face aux rapports entre technique et société de Madeleine Akrich¹⁰³⁸ ainsi que le principe d'une lecture anthropologique de la technique comme élément d'interdépendance internationale avec Marcel Mauss¹⁰³⁹. Ce chapitre s'était également penché sur les rapports entre information et matérialité ainsi qu'entre information et progrès technique, ainsi que sur les représentations de la technique par le biais des fictions chez Lucien Sfez¹⁰⁴⁰. Il ne s'agit pas ici de revenir sur ces aspects déjà évoqués de la sociologie des sciences et techniques pour comprendre un phénomène du langage mais de rechercher l'apport sociologique à la définition des technologies de l'informations proposées par les théories des Relations Internationales.

Si on se réfère à l'ouvrage collectif intitulé *Technology and World Politics an Introduction* dirigé Daniel McCarthy en 2018¹⁰⁴¹, il y a quatre approches des sociologies des sciences et techniques qui peuvent être retenue en Relations Internationales et qui constituent autant de portes de sortie pour quitter le déterminisme technique des relations internationales : la construction sociale des technologies, la théorie de l'acteur-réseau, la théorie critique de la technologie et le post-humanisme¹⁰⁴².

1 – Théorie critique des technologies : penser le développement inégal et la domination.

Dans son ouvrage collectif de 2018, Daniel McCarthy discute de la possibilité d'une théorie critique des technologies¹⁰⁴³. Après une brève relecture de la philosophie de Marx et

¹⁰³⁸ Cette typologie rangeait les approches selon qu'elle partait du principe que la technique était autonome par rapport au monde social, que l'une construisait l'autre, ou qu'elles se coconstruisaient de façon réticulaire. AKRICH Madeleine, 1987, op-cit. ainsi que AKRICH Madeleine, 1994, op-cit.

¹⁰³⁹ DURKHEIM Emile et MAUSS Marcel, 1913, op-cit. ; MAUSS Marcel, 1930 op-cit.

¹⁰⁴⁰ SFEZ Lucien, 2002, op-cit.

¹⁰⁴¹ MCCARTHY Daniel R. ; MCCARTHY, Daniel R. (dir), 2018, op-cit. pp. 24 – 102.

¹⁰⁴² D'autres approches sociologiques à la rencontre du matériel et du social sont intéressantes, mais n'ont pas été retenue dans cette partie. A titre d'exemple, il est également possible de penser aux travaux de Lucy Suchman sur le champ théorique de « l'action située » ou « cognition située ». Ces recherches étudient les interactions entre les utilisateurs et les artefacts technologiques. SUCHMAN Lucy, A. *Plans and situated actions: The problem of human-machine communication*. Cambridge university press, 1987. Sur les débats et l'évolution de cette théorie, voir la synthèse QUERE Louis., « La situation toujours négligée ? », *Réseaux*, volume 15, n°85, 1997, pp. 163-192. Il est également possible de penser à la sociologie des usages. Voir la synthèse PROULX Serge. « La Sociologie Des Usages, Et Après ? » *Revue Française Des Sciences De l'Information Et De La Communication*, n°6, Janvier 2015.

¹⁰⁴³ MCCARTHY Daniel R. « Critical Theory of Technology Design, domination and uneven development » In. MCCARTHY Daniel R. (dir.), 2018, op-cit, pp. 60 – 83.

Engels associant technologies et forces de production. L'auteur se pose la question ontologie de la technique : est-elle une structure de domination ou un instrument de libération ? Cette question donne lieu à un tour d'horizon des approches marxistes de la technologie.

Parler de théorie critique des technologies ne va pas forcément de soi en Relations Internationales. En effet, bien que la théorie possède des racines dans la pensée de Marx, elle ne s'est que rarement penchée sur les technologies dans les Relations Internationales¹⁰⁴⁴. De manière générale la théorie critique des Relations Internationales associe une attention soutenue à l'économie politique et la dynamique complexe du pouvoir culturel découlant d'inégalités structurelles persistantes. Dès lors, elle peut représenter une théorie intéressante pour analyser les technologies. Toutefois, pour y arriver, elle doit faire appel à la sociologie historique, ainsi qu'aux apports des auteurs de la théorie critique en dehors des Relations Internationales¹⁰⁴⁵.

Pour Daniel McCarthy, l'auteur à retenir pour construire une théorie critique des technologies en Relations Internationales est Andrew Feenberg¹⁰⁴⁶.

« La technologie peut être réorganisée tant que les machines développées sous le capitalisme sont utilisées pour produire une nouvelle génération de machines adaptées aux objectifs socialistes. Le pouvoir de classe détermine laquelle des potentialités ambivalentes du patrimoine sera réalisée. »¹⁰⁴⁷.

Selon Feenberg, un artefact technologique n'est pas seulement un outil. La forme qui lui est donnée lors de sa conception détermine les possibilités de l'utilisateur de s'en servir. Les objets sont biaisés en tant que produit de leur conception, créés pour atteindre certains objectifs

¹⁰⁴⁴ Pour deux contre-exemples, sur les États-Unis après la deuxième guerre mondiale : RUPERT Mark. *Producing Hegemony: the Politics of Mass Production and American Global Power*. Cambridge University Press, 1995, 280 p. ; VAN DER PIJL Kees, (1984) *The Making of an Atlantic Ruling Class*, Verso Books, 2012, 331 p.

¹⁰⁴⁵ Parmi tous les auteurs cités ayant l'apport le plus intéressant sur la technologie, il faut sans doute retenir les travaux de Max Horkheimer, d'Herbert Marcuse et Jürgen Habermas. Nous avons déjà évoqué les travaux des deux derniers sur la technique (Chap. 1). Horkheimer a une pensée qui évolue davantage entre les années 20 et les années 40. Si pour lui la technologie est un moyen d'émancipation au départ dans sa thèse en 1922, elle deviendra un moyen d'oppression en 1947 dans son ouvrage avec Adorno. Pour la version française : HORKHEIMER Max et ADORNO Theodor W. (1947), *La Dialectique De La Raison: Fragments Philosophiques*. Gallimard, 1974, 281 p.

¹⁰⁴⁶ D'une part, pour son commentaire du débat entre Marcuse et Habermas sur la question de la technologie. FEENBERG Andrew, « Marcuse or Habermas: Two critiques of technology », *Inquiry*, vol. 39, n°1, 1996, pp. 45-70. D'autre part pour ses ouvrages consacrés à la théorie critique de la technologie. FEENBERG Andrew, *Transforming Technology a Critical Theory Revisited*. Oxford Univ. Press, 2002, 232 p. et FEENBERG Andrew, *Between Reason and Experience: Essays in Technology and Modernity*, MIT Press, 2010, 284 p.

¹⁰⁴⁷ FEENBERG Andrew, 2002, op-cit. p.53. (Notre traduction)

et non d'autres¹⁰⁴⁸. Ces objets technologiques biaisés aident à reproduire et perpétuer le système social qui les a conçus. Toutefois, Feenberg suggère que leur futur ambivalent permet la réalisation de possibilités politiques alternatives. Il y a donc une part de déterminisme technique dans la pensée de l'auteur (technologie biaisée par essence) qui se combine avec le libre arbitre conceptualisé autour de l'ambivalence de la technologie.

En se basant sur la théorie de Feenberg, Daniel McCarthy propose une application de la théorie critique des technologies aux Relations Internationales. Cette proposition repose sur le postulat que la technologie n'est pas déterminée à l'intérieur des frontières de l'État mais un produit issu de la sphère internationale. Le but de cette théorie n'est pas de rendre compte de l'ensemble des politiques des technologies à l'échelle internationale mais d'analyser comment l'idéologie et les asymétries structurelles du pouvoir façonnent les ordres socio-techniques.

« La théorie critique de la technologie en RI fournit un compte-rendu de la politique de la technologie dans laquelle la sensibilité au contexte historique et aux trajectoires spécifiques d'artefacts et de systèmes technologiques individuels se combine avec un compte macro-sociologique de la modernité. Comme pour la théorie des RI critiques en général, elle évite l'aspect historicisme et le statocentrisme de la théorie des RI classiques. Il souligne comment des luttes de pouvoir spécifiques sur la configuration précise de la technologie, menée entre classes et États, permettent et maintiennent des hiérarchies sociales (pas simplement des hiérarchies entre États) dans la politique globale. Il pointe également vers une critique normative de ces pratiques globales. »¹⁰⁴⁹

Dans le système capitaliste, le droit de diriger le processus de développement technologique détenu par les propriétaires privés est garanti par l'État. Cependant, la pluralité des communautés politiques à l'échelle internationale impacte la technologie de manières différentes. Ces communautés se développent inégalement du fait de la concurrence technologique entre les différents ensembles régaliens. A cette assertion sur le développement, McCarthy ajoute une dimension comparative.

¹⁰⁴⁸ MCCARTHY Daniel R, 2018, op-cit. p. 69.

¹⁰⁴⁹ Ibid. p. 78. (Notre traduction)

« Cette dimension comparative de la politique mondiale ne doit pas être sous-estimée. La technologie est souvent un point central de comparaison entre les communautés nationales, imprégnant ainsi les cultures nationales d'un sentiment de supériorité ou d'infériorité. »¹⁰⁵⁰

Il est important de souligner ici que ce modèle ne concerne pas uniquement les technologies de l'information, mais concerne l'ensemble des secteurs dans lesquels sont produits des artefacts technologiques. Ce qui permet d'étendre cette théorie à la sécurité, au travers des technologies de l'armement. Néanmoins, la sécurité de l'information n'est directement pas évoquée.

2 – Construction sociale des technologies de l'information et Relations Internationales.

La première approche que nous retiendrons ici est celle de la construction sociale des technologies de l'information. L'application de cette théorie aux Relations Internationales découle de trois travaux fondateurs. Dans l'ordre chronologique, les premiers travaux sont relatifs au développement de la théorie du constructivisme social. Les deuxièmes à l'application du constructivisme aux sciences et technologie créant la construction sociale des technologies (désignée dans la littérature sous l'acronyme SCOT)¹⁰⁵¹. Les troisièmes à l'application du constructivisme social aux Relations Internationales¹⁰⁵².

En résumé, le principe de la construction sociale des technologies veut que l'on s'intéresse à l'analyse sociologique d'un artefact afin de démontrer sa flexibilité interprétative, notamment de manière à décrire la construction sociale et de l'expliquer en tenant compte des différences de contextes technologiques entre les groupes sociaux. Dans sa forme originale, ce modèle s'intéressait surtout aux technologies massivement produites.

Un exemple de travaux qui pourraient s'inscrire dans ce cadre, est la vision constructiviste des technologies de l'information comprises comme « système sociotechnique »

¹⁰⁵⁰ Ibid. p.74 (Notre traduction)

¹⁰⁵¹ PINCH Trevor J. et BIJKER Wiebe E., 1987, op-cit.

¹⁰⁵² WENDT Alexander, 1992, op-cit ; WENDT Alexander, 1999, op-cit.

développée par Geoffrey Herrera en 2003¹⁰⁵³. Dans cette approche, la technologie est politique par nature car non seulement sa construction est un sujet de contestation politique, mais également selon l'auteur, car la technologie est un genre de connaissances pratiques, intégrées à des artefacts matériels, dans des institutions construites pour les gérer, elles-mêmes interfacées avec les autres institutions sociales¹⁰⁵⁴. Cette approche se réclame de la construction sociale des technologies¹⁰⁵⁵ et de l'histoire sociale des idées. Elle repose sur l'idée que la technologie est une institution socio-politique combinée avec la théorie de la capacité d'interaction de Buzan et Little¹⁰⁵⁶. L'ontologie qui en émerge vise à considérer la technologie comme la construction d'institutions sociotechniques complexes en tant que processus politique international. Un large système sociotechnique définit un médium d'interaction entre les acteurs des Relations Internationales. Les technologies apparaissent dans un entre-deux intégrant déterminisme et construction. La technologie est construite par le social et détermine un certain nombre d'effet sociaux. Elle est un produit sociotechnique de l'intérêt humain mais lui résiste. Afin de sortir de ce dilemme, l'article propose d'introduire la dimension temporelle et notamment le cycle de vie des systèmes sociotechniques qui permet de discriminer l'impact d'une technologie à différent moment de son cycle de vie. Autrement dit, elle se concentre principalement sur le développement et la diffusion de la technologie. La discussion utilise plusieurs artefacts que sont la poudre à canon, le journal, le chemin de fer, les armes nucléaires et les technologies de l'information. Geoffrey Herrera poussera l'analyse plus loin en 2006 avec l'ouvrage *Technology and International Transformation*¹⁰⁵⁷.

L'auteur emploie beaucoup l'idée de système. Néanmoins le système fait davantage figure d'une notion que d'un concept ici. Selon Mary Manjikian¹⁰⁵⁸, l'apport de la construction sociale des technologies peut être identifié dans quatre concepts : le *momentum*, la *path*

¹⁰⁵³ HERRERA Geoffrey L. 2003, op-cit.

¹⁰⁵⁴ Ibid p 560.

¹⁰⁵⁵ On retrouve ici des éléments de l'ouvrage BIJKER Wiebe E, HUGHES Thomas P. et PINCH Trevor J. (eds.), 1987, op-cit. même s'il n'y est pas fait explicitement référence dans l'article.

¹⁰⁵⁶ Voir BUZAN Barry, LITTLE Richard, et JONES Charles, 1993 op-cit. ainsi que BUZAN Barry et LITTLE Richard, 2001, op-cit.

¹⁰⁵⁷ HERRERA Geoffrey L., *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*, New York, SUNY Press, septembre 2006, 275 p. La typologie du changement dans le système international (p. 6 – 8) est particulièrement intéressante.

¹⁰⁵⁸ MANJIKIAN Mary, « Social construction of technology How objects acquire meaning in society » In. McCARTHY, Daniel R. (dir.), 2018, op-cit, pp. 25 – 41.

dependence, les saillances inversées et l'avantage du premier entrant (ou avantage pionnier). L'ensemble de ces concepts s'inscrit dans le courant constructiviste du fait qu'ils permettent de nourrir le débat sur l'agentivité des Relations Internationales. Avec ces quatre concepts, la construction sociale des technologies fournit une grille d'analyse de moyenne portée capable d'articuler le déterminisme technique et le détermination sociale des techniques.

Défini par Thomas Hughes¹⁰⁵⁹, le *momentum* technologique est une théorie qui décrit l'influence réciproque et inscrite dans le temps de la société et de la technologie. La technologie est ainsi un large système (*Large technical system*) intégrant une composante humaine et une composante technique. La technologie évolue grâce à ses deux composantes dont les forces évoluent dans le temps. Selon l'auteur, plus un système vieilli plus la technique y tient une place forte.

Le déterminisme technique est donc moins un effet ordinaire de la technique que le signe d'un système technique vieillissant (donc moins adaptable). Attention cependant à ne confondre les systèmes techniques et l'artefact lui-même. Un artefact technologique comme un ordinateur ou un téléphone portable est composé par plusieurs systèmes techniques. Le *momentum* est une sorte d'agrégat composé de plusieurs éléments hiérarchisés.

« Un système avec un *momentum* important a une masse, une vitesse et une direction. Dans le cas des systèmes technologiques [...] la masse consiste en machines, dispositifs, structures et autres artefacts physiques dans lesquels un capital considérable a été investi. Le *momentum* découle également de la mise en place de compétences personnelles en matière de planification et de gestion de la performance. Les entreprises, les administrations publiques, les sociétés de presse, les institutions éducatives et les institutions de formation, ainsi que les organisations de formation, [...] Prises ensemble, les organisations impliquées dans le système peuvent être décrites en tant que culture du système. Un système avec une telle masse a généralement un rythme perceptible de croissance ou de la vitesse. [...] Un système est généralement une direction, ou des objectifs. La définition des objectifs est plus importante dans un système jeune que pour un système ancien, dans lequel le *momentum* produit de l'inertie »¹⁰⁶⁰

Les différentes vitesses de développement des sous-systèmes peuvent créer des « saillances inversées » qui peuvent entraver le *momentum* d'un système. En conséquence, les

¹⁰⁵⁹ Voir HUGHES Thomas P., *Networks of Power: Electrification in Western Society, 1880-1930*, Baltimore: Johns Hopkins University Press, 1983, 476 p. ; HUGHES Thomas P., 1987, op-cit.

¹⁰⁶⁰ HUGHES Thomas P., 1983, op-cit. p. 15. (Notre traduction).

avancées technologiques de l'ensemble du dispositif peuvent être impactées par des limitations technologiques ou par des avancées au sein d'un sous-système constituant. Ces saillances inversées peuvent être des composants techniques ou sociaux du système. Une mesure abondante de l'écart de performance de la saillance inversée a été introduite par les travaux de Ozgur, Dedehayire et Saku Mäkineif.¹⁰⁶¹. Cette mesure repose sur la différence de performance technologique à la saillance et la saillance inversée inscrite dans le temps.

La dépendance au sentier (*path dependence*) est un concept importé des sciences économiques par Paul Pierson¹⁰⁶². Il trouve à s'appliquer dans le domaine de la construction sociale de la technologie afin de conceptualiser la restriction des choix possibles du fait des décisions antérieures. Cette théorie veut que toute institution et tout choix politique produisent des dynamiques « auto-renforçantes » une fois installé et opère une fois de restriction de la liberté de choix.

Le dernier concept proposé est l'avantage pionnier¹⁰⁶³ où le premier acteur a avoir opté pour un choix technologique dispose d'un avantage concurrentiel qui se prolonge dans le temps. Cet avantage tient en deux éléments : d'une part, il accomplit quelque chose que les autres acteurs ne font pas, mais d'autre part, l'acteur dispose initialement d'une plus grande liberté technologique et il peut réduire celle des autres acteurs en verrouillant la technologie. S'assurant une position dominante dans son environnement.

Cette grille conceptuelle forme le cœur de la construction sociale des technologies. Elle se concentre prioritairement sur l'influence de la technologie dans la détermination du politique. Néanmoins, la réception de cette grille dans les Relations Internationales nourrit une opposition entre le constructivisme classique et ses pendants radicaux. Ces derniers ne sont pas tant intéressés par la dimension matérielle de la technologie que par son côté symbolique et

¹⁰⁶¹ DEDEHAYIR Ozgur et MÄKINEIF Saku J., « Dynamics Of Reverse Salience As Technological Performance Gap: An Empirical Study Of The Personal Computertechnology System. » *Journal of Technology Management & Innovation*, vol. 3, no. 3, 2008, pp. 55 – 66.

¹⁰⁶² PIERSON Paul. « Increasing returns, path dependence, and the study of politics. », *American political science review* vol. 94 n° 2, 2000, pp. 251-267.

¹⁰⁶³ Concept également issus des sciences économiques, LIEBERMAN Marvin B. et MONTGOMERY David B.. « First-Mover Advantages. » *Strategic Management Journal*, vol. 9, no. S1, 1988, pp. 41–58

performatif. Néanmoins l'une et l'autre ne sont pas forcément inscrites dans une dimension technophile ou technophobe.

« Toutes deux soulignent que les objets technologiques se développent au sein de systèmes où les concepteurs et les régulateurs ont une certaine autorité, mais ne jouissent pas d'un monopole pour dicter la manière dont une technologie apparaît ou fonctionne dans la société. »¹⁰⁶⁴

3 – Nouveaux matérialismes : réalisme spéculatif, post-humanisme et philosophie orientée objet.

Notre troisième ensemble de théories pousse plus loin les limites dans la critique de la séparation entre le monde social et la technologie. Ce sont les « nouveaux matérialismes »¹⁰⁶⁵. L'appellation est assez large et regroupe de nombreux travaux¹⁰⁶⁶. Nick Srnicek identifie néanmoins plusieurs traits communs entre toutes ces approches : le rapport privilégié avec les sciences naturelles, la télologie du dépassement de la distinction entre la nature et l'humain et donc du déterminisme présent dans les théories classiques des relations internationales. Elles rejettent également le caractère anthropocentrique de ces mêmes théories, et reconnaissent l'apport d'éléments non-humains à la vie sociale (ce qui remet également en cause la distinction entre l'humain et le non-humain)¹⁰⁶⁷.

Du point de vue philosophique, ces théories remettent en question la stabilité d'un sujet libéré individualisé et préconisent une attention matérialiste critique aux influences globales.

¹⁰⁶⁴ MANJIKIAN Mary, 2018, op-cit. p. 39. Pour une approche constructiviste radicale, notamment sur les problématiques des usages nouveaux non prévus dans la conception technologique, voir par exemple GRINT Keith et WOOLGAR Steve. « On Some Failures of Nerve in Constructivist and Feminist Analyses of Technology. » *The Gender-Technology Relation*, 1995, pp. 48–75. Voir également, WOOLGAR Steve et LEZAUN Javier, « The Wrong Bin Bag: A Turn to Ontology in Science and Technology Studies? », *Social Studies of Science*, vol. 43, no. 3, juin 2013, pp. 321–340,

¹⁰⁶⁵ Pour l'application aux Relations Internationales, voir SRNICEK Nick, « New materialism and posthumanism », In MCCARTHY, Daniel R. (dir.), 2018, op-cit. pp. 84 - 101. Voir également, COOLE Diana, « Agentic Capacities and Capacious Historical Materialism: Thinking with New Materialisms in the Political Sciences ». *Millennium: Journal of International Studies*, vol. 41 n°3, 2013, pp. 451– 469 ; Voir enfin : DOLPHIJN Rick, et TUIN (van der) Iris, *New Materialism: Interviews & Cartographies*, Ann Arbor, Open Humanities Press, 2012, 200 p.

¹⁰⁶⁶ Il est d'ailleurs particulièrement difficile d'être exhaustifs sur le sujet, se revendiquent des nouveaux matérialismes certains théoriciens féministes, mais l'on retrouve aussi ce label dans les études environnementales, dans la théorie queer, dans la sociologie des sciences, dans la philosophie (notamment inspirée par Michel Foucault et Giles Deleuze), et dans de nombreux autres domaines. Ce champs entretient ainsi une vaste pluralité d'approches méthodologiques.

¹⁰⁶⁷ SRNICEK Nick, op-cit. pp. 84-86.

Cela peut se traduire par diverses remises en cause allant de l'ontologie de certains phénomènes sociaux, jusqu'au rejet de l'État au profit de l'étude du quotidien, ou des questionnements épistémologiques sur le changement et la contingence. Nick Srnicek met en avant trois terrains d'apports de ces approches en Relations Internationales : les études sur les corps, les neuropolitiques et les politiques de la connaissance, et enfin le posthumanisme¹⁰⁶⁸.

En 2015, Lauren Wilcox, écrit sur les réflexions sur la violence contre les corps dans le domaine des Relations Internationales. Les corps peuvent servir d'objet d'étude en articulant la manière dont les corps sont façonnés et façonnent la violence ou la manière dont ils sont racisés ou genrés avec les effets politiques que cela produit. Le corps est ici une forme d'entité matériel préexistant au politique¹⁰⁶⁹. Il est évidemment possible de penser au genre et aux études féministes. Mais le lien entre l'armée, la guerre et les corps semble également pouvoir constituer un objet d'études intéressant les Relations Internationales¹⁰⁷⁰. Dans les approches de ce type, la technologie, et plus encore la technique, sont toutes deux synonymes de violence envers les corps¹⁰⁷¹.

Du point de vue des neuropolitiques, Nick Srnicek fait appel aux travaux de William Connolly sur les liens entre cerveau et les affects avec le politique¹⁰⁷². Ces affects sont ontologiquement considérés comme la source de nos émotions, désirs et intuitions. Ce socle forme la base du (micro)politique. C'est une théorie intéressante en ce qu'elle permet notamment de fonder l'analyse de la charge affective de l'identité. Toutefois, l'article cité ne fait nullement référence aux technologies de l'information ou la technique, il sera donc écarté.

Le dernier apport des néo-matérialismes concerne le post-humanisme. Cet apport se base sur les travaux d'Erika Cudworth et Stephen Hobden concernant les systèmes complexes,

¹⁰⁶⁸ Ibid. p. 86.

¹⁰⁶⁹ WILCOX Lauren B. *Bodies of Violence: Theorizing Embodied Subjects in International Relations*. Oxford University Press, 2015, 252 p.

¹⁰⁷⁰ En France, le colloque annuel 2019 de l'Association pour les Etudes sur la Guerre et la Stratégie (AEGES) a pour thématique « Corps et guerre ».

¹⁰⁷¹ Voir par exemple : PROTEVI, John, *Life, War, Earth: Deleuze and the Sciences*. University of Minnesota Press, 2013, 264 p

¹⁰⁷² CONNOLLY William E., « The ‘New Materialism’ and the Fragility of Things. » *Millennium: Journal of International Studies*, vol. 41, no. 3, 2013, pp. 399–412.

ainsi que ceux de Diana Coole sur l'agentivité¹⁰⁷³. L'enjeu est de démontrer l'apport du post-humanisme dans le dépassement des limites entre acteurs humains et non-humains dans la définition des acteurs des Relations Internationales. Nous reviendrons sur cette distinction au moment d'aborder la question de l'agentivité.

Bien qu'elles aient globalement assez peu d'apports sur la question de la technologie en tant que telle (exception faites du corp), l'ensemble des théories invoquées au titre des nouveaux matérialismes apportent de nombreux éléments intéressants les Relations Internationales dans les domaines de l'identité, de l'agentivité ou de la dimension concrète du politique. Ces théories constituent des pistes intéressantes pour approfondir le phénomène de la sécurité de l'information au-delà du discours.

4 – Théorie de l'acteur-réseau et technologie dans les Relations Internationales.

La dernière théorie qu'il nous reste à évoquer pour prendre en compte le phénomène technologique dans les Relations Internationales est la théorie de l'acteur-réseau (*Actor-Network Theory*). Nous avons déjà évoqué la théorie de l'acteur-réseau sous la dénomination de sociologie de la traduction avec Madeleine Akrich, Bruno Latour et Michel Callon au moment d'évoquer les postures intellectuelles face à la technique¹⁰⁷⁴. La finalité initiale de la théorie de l'acteur-réseau vise la fabrication scientifique des faits.

« La théorie de l'acteur-réseau a commencé avec la notion de traduction que j'ai empruntée à Michel Serres, au milieu des années 70. Il s'agissait pour moi de comprendre comment des connaissances scientifiques circulaient, en partant de l'idée très simple que c'est au moment de la formulation des problèmes, quels que soient leurs contenus, que se dessinent les espaces de circulation : mon premier texte de 1974 portait sur l'opération de traduction et la mise en réseau des problèmes. Cela permettait d'éviter aussi bien la scolastique des champs ou des sphères sociales que les contractions entre analyse de contenu et analyse de contexte. Je pense que la notion de traduction est la plus générale et la mieux

¹⁰⁷³ En particulier sur l'ouvrage : CUDWORTH Erika et HOBDEN Stephen, *Posthuman International Relations: Complexity, Ecologism and Global Politics*, New York, Zed Books Ltd, avril 2013, 224 p. ; COOLE Diana, 2013, op-cit.

¹⁰⁷⁴ Cf. chapitre 1. ; AKRICH Madeleine, CALLON Michel et LATOUR Bruno (éd.), 2006, op-cit.

adaptée. Malheureusement, un peu plus tard, j'ai introduit cette étrange expression en forme d'oxymore : acteur-réseau. Et c'est elle qui, à mon grand désespoir, a été retenue. »¹⁰⁷⁵

Depuis son invention dans les années 80¹⁰⁷⁶, de nombreux auteurs sont intervenus pour enrichir et préciser la théorie¹⁰⁷⁷. En tant que théorie, l'acteur-réseau repose sur peu de postulats ontologiques semblables à ceux des Relations Internationales. Ici, la théorie opte pour une définition des concepts à partir des recherches empiriques plutôt qu'à partir d'un postulat ontologique. Le concept qui aurait une valeur fondamentale serait celui de réseau. En résumé, dans cette théorie, le réseau est une méta-organisation comprenant des humains et des non-humains¹⁰⁷⁸. L'objet de réseau peut s'appliquer à tous les ensembles sociaux (organisation, pratique, sphère d'activité, institution, processus, etc.). Le social est ainsi le produit des interactions successives d'actants hétérogènes (humains ou non).

L'acteur-réseau est grevé d'une forme d'agentivité collective qui évolue dans le temps et opère suivant une série de fabriques de sens qui ordonne le réseau et y produisent une forme d'intelligibilité. Ce processus est conceptualisé comme une traduction qui produit un fait scientifique stable à partir d'une situation de controverse au sein du réseau. L'étude des associations produite par la traduction ainsi que de l'évolution du réseau est le travail essentiel que permet cette grille de lecture. Il est important de préciser que l'agentivité ne peut se réaliser qu'au travers du réseau. Dans cette théorie, un acteur désigne n'importe quel élément qui « cherche à courber l'espace autour de lui, à rendre d'autres éléments dépendants de lui, à

¹⁰⁷⁵ CALLON Michel, et FERRARY Michel. « Les réseaux sociaux à l'aune de la théorie de l'acteur-réseau », *Sociologies pratiques*, vol. 13, n°2, 2006, p. 41.

¹⁰⁷⁶ Pour les quatre textes fondateurs : LATOUR Bruno, et WOOLGAR Steve. *La Vie De Laboratoire La Production Des Faits Scientifiques*. Paris, Editions La Découverte, 1979, 271 p. ; LATOUR Bruno, *Les Microbes: Guerre Et Paix ; Suivi De: Irréductions*. A.M. Métailié, 1984, 281 p. CALLON Michel, « La domestication des coquilles Saint-Jacques et des marins-pêcheurs dans la baie de Saint-Brieuc », *L'année sociologique*, n°36, 1986, pp. 169-208 ; AKRICH Madeleine, 1987, op-cit. ; Pour le texte le plus ancien, voir également : CALLON Michel et LATOUR Bruno, « Unscrewing the Big Leviathan: how actors macrostructure reality and how sociologists help them to do so », in KNORR-CETINA Karin D. et CICOUREL Aaron V. (éds.), *Advances in Social Theory and Methodology: Toward an Integration of Micro- and Macro-Sociologies*, Boston, Mass, Routledge and Kegan Paul, pp. 277-303.

¹⁰⁷⁷ Pour une étude des travaux intéressants les Relations Internationales sur la théorie de l'acteur-réseau, voir BUEGER Christian et STOCKBRUEGGER Jan., « Actor-Network Theory Objects and actants, networks and narratives », In MCCARTHY, Daniel R. (dir.), 2018, op-cit, pp.42 - 59.

¹⁰⁷⁸ Une des applications du principe de symétrie de la théorie de l'acteur-réseau implique de placer sur un même plan épistémologique les sujets humains et les objets non-humains qui peuvent tous accéder à une forme de d'agentivité. Cette équivalence entre le sujet et l'objet est l'un points d'intérêts de cette théorie et également l'un des plus critiqués.

traduire les volontés dans le langage de la sienne propre »¹⁰⁷⁹. L'actant, lui, a la capacité d'agir et d'influencer les choses. C'est donc une notion plus large que celle de l'acteur qui contrairement à lui ne dépend pas du réseau pour exister. Le « traducteur » est un acteur qui aide la construction du lien qui relie les membres de ces entités hétérogènes qui constituent un réseau. Du point de vue des technologies, un autre concept intéressant ici est celui de « médiateur ». Un médiateur est un actant constitué par une technologie animée d'un pouvoir de transformation des enjeux qu'elle porte.

Dans son article de 2012¹⁰⁸⁰, Andrew Barry s'interroge sur les relations entre la théorie de l'acteur-réseau et les Relations Internationales. Le but est ici de savoir si la théorie est applicable ou non aux Relations Internationales. Il définit la traduction comme ayant trois caractères particuliers : une forme d'exercice du pouvoir (politique), impliquant un mouvement dans l'espace et une transformation de l'espace (géographique), et qui constitue tout autant un processus d'imitation que de différenciation (littéraire)¹⁰⁸¹. La traduction apparaît ainsi en tant que processus politique animé par ses propres règles et sources de contestation. En 2006, Emily Apter met au point le concept de « zone de traduction » (*translation zone*)¹⁰⁸² afin de pointer les résistances à la traduction notamment linguistiques.

Du point de vue des Relations Internationales, il existe plusieurs enjeux importants¹⁰⁸³. Le premier intérêt de cette théorie en Relations Internationales réside dans le fait qu'elle permet de traiter les institutions et les discours mais aussi les pratiques politiques et l'expertise sur un même plan. Cela facilite l'inclusion de « nouveaux » objets dans le champ des Relations Internationales. Cela pose également la question de l'évolution de la distinction entre le politique et le non-politique. Le secret qui entoure les Relations Internationales a pu conduire la théorie des réseaux d'acteurs à être critiquée pour sa superficialité et pour son incapacité à interroger les structures de relations censées se trouver sous la surface. Cela nous semble être

¹⁰⁷⁹ CALLON Michel et LATOUR Bruno, *La science telle qu'elle se fait. Anthologie de la sociologie des sciences de langue anglaise*, Paris, La Découverte, 1991, p. 20

¹⁰⁸⁰ BARRY Andrew, « The Translation Zone: Between Actor-Network Theory and International Relations », *Millennium: Journal of International Studies*, 41, 3, 2012, pp. 413-429.

¹⁰⁸¹ Ici, il est possible de faire un parallèle avec la sociologie de l'imitation de Gabriel Tarde. Cf. Chapitre 1.

¹⁰⁸² APTER Emily, *The Translation Zone*, Princeton, Princeton University Press, 2006, 225 p.

¹⁰⁸³ BARRY Andrew, 2012, op-cit. pp. 422 – 429.

une critique mal fondée dans la mesure l'indisponibilité des faits et des sources n'est pas propre à une théorie scientifique. Elle inhérente au domaine étudié et affecte tous les chercheurs peu importe leur positionnement épistémique. Le dernier domaine concerne les circonstances historiques ou de la contingence de la politique internationale. Andrew Barry propose ici de tourner la théorie de l'acteur-réseau vers l'analyse des situations politiques¹⁰⁸⁴. Une situation politique doit ici être comprise comme le point de rencontre de divers courants et mouvements d'idées et de pratiques, de croyances et de désirs, qui se confondent dans des contextes particuliers ou dans le temps¹⁰⁸⁵. Ces situations ne sont pas simplement discursives mais sont des construits (ou des assemblages) d'artefacts de diverses natures, où les discours se rejoignent par des artefacts technologiques et matériels. Ajoutons que cela est possible grâce au concept de médiateur¹⁰⁸⁶. Enfin une situation politique est par nature incertaine, ambiguë et contestée. Dès lors, il n'y a pas d'analyse politique définitive de ces situations de conflits¹⁰⁸⁷.

Ainsi nous avons évoqué quatre manières de résoudre la difficulté de compréhension des technologies dans les Relations Internationales : la théorie critique, la construction sociale des technologies, les nouveaux matérialismes et la théorie de l'acteur-réseau. Bien que notre préférence aille à la théorie de l'acteur-réseau qui a le mérite d'avoir beaucoup des avantages des autres méthodes et d'être compatible avec elles, une compréhension satisfaisante de la technologie passera immanquablement par une approche multidimensionnelle voire pluridisciplinaire.

C – La question de l'agentivité : pluralité et diversité des acteurs.

La question de l'agentivité (*agency*) est une vieille question des Relations Internationales que nous aurons sans doute grande peine à résumer ici. L'agentivité désigne la qualité d'acteur (ou d'agent), qui permet à ce dernier d'exister du point de vue des Relations

¹⁰⁸⁴ IBID.

¹⁰⁸⁵ Nous faisons le lien ici avec la sociologie de Jean-Claude Passeron et tout particulièrement, le concept de monde historique. Cf. chapitre liminaire.

¹⁰⁸⁶ Cf. supra.

¹⁰⁸⁷ Ici nous pouvons faire un parallèle avec le texte explicatif idéal de la méthodologie de Jérémie Cornut et le rejet de la logique popérienne de réfutation de Passeron. Cf. encore une fois au chapitre liminaire.

Internationales. Cela se manifeste dans la reconnaissance d'une capacité à agir ou à influencer la politique internationale.

Plusieurs débats ont cours pour connaître les limites de cette agentivité. Derrière la simple question de l'analyse, certains auteurs y voient un enjeu épistémologique majeur qui touche à l'existence de la discipline des Relations Internationales. Nous reviendrons sur les contours de l'agentivité d'un point de vue théorique avant d'explorer l'impact de la sécurité de l'information sur celle-ci.

1 – Les contours de l'agentivité en Relations Internationales.

Savoir quels sont les acteurs pertinents pour analyser les Relations Internationales est un problème complexe qui implique deux interrogations principales¹⁰⁸⁸. Ces questions sont principalement celles du niveau d'analyse et le problème agent-structure.

La première question est d'apparence plutôt simple. Afin d'éviter la question du bon (concept d') acteur, les auteurs ont eu tendance à découper la discipline en niveau d'analyse. Si bien que cette partition est devenue relativement commune dans les Relations Internationales et malgré le développement des approches multiniveaux, il y a une forme césure entre les méthodes et les concepts pour aborder chacune des dimensions des Relations Internationales (un point que la combinaison pragmatique pourra sans doute résoudre). D'une vision de l'agentivité particulièrement stato-centrée au départ, la discipline s'est vue rapidement proposer d'autres théories qui ouvrent la porte à d'autres acteurs. Parmi les principaux travaux, se trouvent ceux de Kenneth Waltz qui propose un modèle à trois niveaux d'analyse : l'individu, l'État et le système international¹⁰⁸⁹. Par ailleurs, il y a une tentation certaine lorsqu'on travaille sur le cyberspace à employer une version contemporaine du *cobweb model* de Burton¹⁰⁹⁰. Le

¹⁰⁸⁸ BRAUN Benjamin, SCHINDLER Sebastian et WILLE Tobias. « Rethinking agency in International Relations: performativity, performances and actor-networks. », *Journal of International Relations and Development*, février 2018, pp. 1-21.

¹⁰⁸⁹ Tout particulièrement dans l'ouvrage tiré de sa thèse de doctorat : WALTZ Kenneth (1959), *Man, the State, and War*, Columbia University Press, 2001, 263 p.

¹⁰⁹⁰ Lequel propose un modèle de toile d'araignée centré sur l'individu où chaque fil représente les relations qui unissent les différentes unités de systèmes (notamment en étudiant les communications) jusqu'à former une immense toile d'araignée couvrant toute la planète. Ce modèle est à la fois opposé à une vision traditionnelle par les cartes des Relations Internationales ainsi qu'au modèle des « boules de billard ». Voir BURTON John, *World Society*, Cambridge, Cambridge University Press, juin 1972, 180 p. (plus précisément pp 35 – 45).

développement de la littérature sur les organisations non-gouvernementales et de l'économie politique internationales ont élargi les barrières de la prise en compte de nouveaux acteurs. Mais la question du niveau d'analyse demeure.

La deuxième question est plus complexe et plus récente dans l'histoire de la discipline. Elle est liée à l'introduction du constructivisme dans la discipline. Il s'agit de savoir si les acteurs produisent la structure sociale ou s'ils sont la production de cette structure. L'approche d'Alexander Wendt est ici de lier les deux en affirmant que les acteurs sont contraints par les structures sociales, mais ont aussi le pouvoir, par leurs actes, de transformer ces mêmes structures¹⁰⁹¹. Cela questionne ici la liberté de l'acteur dans la sphère internationale et donc remet en cause une partie de l'agentivité telle qu'elle était formulée de façon classique autour de la souveraineté des États. Aujourd'hui ces travaux sur l'agentivité bénéficient des apports du poststructuralisme et des études sur la performance (principalement dans une vision discursive de l'agentivité) ainsi que de la théorie de l'acteur-réseau (dans une vision relationnelle de l'agentivité grâce au réseau).

2 – Agentivité, asymétrie et sécurité de l'information.

Comment est-ce que le phénomène analysé dans cette thèse vient alimenter ces débats sur l'agentivité ? Principalement, en formulant des contraintes importantes sur la prise en compte sur acteurs. Si on considère que la sécurité de l'information est un phénomène de Relations Internationales alors l'agentivité doit prendre en compte plusieurs paramètres importants qui l'orientent vers une conception « atomiste » des Relations Internationales devant intégrer de plus en plus d'acteurs. Le cyberspace touche tous les niveaux d'analyse¹⁰⁹².

Il y a tout d'abord la question des nouveaux acteurs sur la scène internationale. Les acteurs pouvant avoir un impact sur la cybersécurité à échelle mondiale sont particulièrement. Certains ont une identité connue et les autres non. Au-delà des agences de cybersécurité, des entreprises et des criminels qui sont les acteurs qui profitent le mieux de ces technologies pour émerger sur la scène internationale. Par ailleurs, le cyberspace est opaque et le comportement de la plupart de ces acteurs sont assez flous en termes d'impact réel sur la scène internationale.

¹⁰⁹¹ WENDT Alexander, 1987, op-cit. p. 360.

¹⁰⁹² Cf. chapitre 2 et section 2 du présent chapitre.

Certains de ces acteurs agissent également de manière latente. La conception de l'agentivité qui en résulte doit donc être en mesure de saisir l'invisible.

L'agentivité doit ainsi tenir compte de nouveaux acteurs tout en ignorant potentiellement leur identité avant enquête. Par ailleurs, il y a aussi la question des menaces hybrides, ainsi que la question des « clusters », sociétés savantes et autres groupes informels tels les CERT qui ont directement un impact sur la sécurité. Cela renvoie à la question moins théorique de l'attribution qui est un enjeu essentiel de la sécurité de l'information, et donc désormais de sécurité nationale. Les nouvelles menaces représentées par le discours engendre un climat de confiance limitée au niveau international.

Ces nouveaux acteurs engendrent de nouvelles asymétries et de nouvelles symétries que l'agentivité doit prendre en compte. Les États ont accès à de nouvelles symétries entre eux qui doivent être intégrées aux facultés des acteurs que reconnaît l'agentivité. Mais on retient surtout le cyberespace pour sa faculté de multiplicateur de force pour que les acteurs les plus faibles puissent agir contre les plus puissants. A la lumière de notre recherche et des travaux déjà menés sur cette question, cette asymétrie doit être considérée comme une faculté d'attaquer, de désobéir ou de se dissimuler face à un acteur plus puissant. Elle dépasse le point de vue militaire et s'applique également aux autres activités qu'elles soient licites ou illicites.

Les asymétries engendrent de nouvelles formes de conflits auxquels ces nouveaux acteurs participent directement en tant que cible ou agresseur ou indirectement du fait du besoin de sécurité engendré par ces conflits. Cette cyber-conflictualité alimente la montée en puissance des enjeux militaires du cyberespace jusqu'à les rendre prioritaires sur les autres impératifs au niveau de l'acteur régional.

Au niveau des organisations internationales, L'État doit partager la décision avec de nombreux acteurs en matière d'information forgeant l'un des systèmes internationaux les plus complexes observés à ce jour (gouvernance d'Internet). Il est possible d'observer une compétition entre les nouveaux acteurs ayant émergé du fait du besoin du cyberespace en terme technique, de sécurité ou de gouvernance. Leur reconnaissance en tant qu'acteur est soumis à

question¹⁰⁹³. Ces nouveaux acteurs tels l'ICANN se livrent à des discussions avec les organisations internationales plus anciennes telles que l'UIT.

Enfin, l'agentivité ne peut pas être spécifique au cyberspace, à Internet ou aux technologies de l'information, car les phénomènes observables se produisent dans une logique d'hybridation entre le numérique et les moyens d'action conventionnels.

D – L'information en tant qu'objet : vers les Relations Internationales « computationnelles ».

Cette dernière question renverse la démarche qui était la notre jusqu'ici dans le but de la pousser plus loin. Plutôt que de vouloir travailler sur l'influence de l'information sur les Relations Internationales, pourquoi ne pas travailler sur les Relations Internationales à partir de l'information ? Cette question constitue l'enjeu des Relations Internationales « computationnelles » (*Computational International Relations*)¹⁰⁹⁴.

Cette branche émergente des Relations Internationales remet au goût du jour les débats sur l'apport de l'informatique à l'étude des Relations Internationales, né avec l'importation des méthodes quantitatives dans la discipline¹⁰⁹⁵. Après avoir détaillé quelques approches de la donnée numérique, les Relations Internationales computationnelles seront abordées sous l'angle de l'enjeu des données numériques.

Akin Ünver distingue cinq grands domaines où l'outil informatique possède une plus-value dans l'étude des Relations Internationales : le texte/langage, la cartographie, la modélisation, la communication et le réseau¹⁰⁹⁶. Au-delà de ces approches, l'article est un

¹⁰⁹³ Cf. chapitre 4.

¹⁰⁹⁴ Le terme « computationnelle » est ici traduit littéralement. Parler de Relations Internationales informatiques insistait trop sur l'un des outils de la méthode plutôt que sur la méthode elle-même. L'expression est ici conçue en miroir des *Computational Social Sciences* dont elles s'inspirent. Voir, ÜNVER Akin H., « Computational International Relations: What Can Programming, Coding and Internet Research Do for the Discipline? », *All Azimuth: A Journal of Foreign Policy and Peace*, vol. 8, n°2, 2019, pp. 157-182. ; ainsi que TABER Charles S., et TIMPONE Richard J.. « Beyond Simplicity: Focused Realism and Computational Modeling in International Relations. » *Mershon International Studies Review*, vol. 40, no. 1, 1996, pp. 41–79.

¹⁰⁹⁵ Cf. chapitre liminaire.

¹⁰⁹⁶ ÜNVER Akin H., 2018, op-cit. pp. 157 – 170.

véritable inventaire d'outils en tout genre destiné à employer l'informatique pour étudier les relations internationales.

Au sujet du langage, l'auteur définit les méthodes informatiques comme permettant de retrouver des informations, d'étudier le langage naturel et de faire de l'extraction d'information. Le chapitre 2 de ce manuscrit serait un bon exemple des méthodes décrites par l'auteur notamment en ce qui concerne l'extraction d'information¹⁰⁹⁷.

La cartographie, entendue au sens géopolitique, est un autre outil à la disposition des chercheurs pour visualiser des données. L'exemple d'outil mentionné est le système d'information géographique (ou GIS). Les chercheurs peuvent utiliser des approches vectorielles sur des cartes en deux dimensions ainsi que des projections matricielles en trois dimensions¹⁰⁹⁸. La modélisation repose un peu sur le même principe. Qu'elle soit inspirée des mathématiques, de la physique ou de la biologie, la modélisation du comportement par des équations permet de simuler de nombreux phénomènes. Cartographie et modélisation sont complémentaires dans le principe de tester des théories.

La communication numérique et les réseaux sont également des outils puissants qui constituent à la fois des objets et des outils d'enquête intéressants pour les chercheurs. Au niveau des enquêtes, Derek Ruths et Jürgen Pfeffer ont ainsi pu démontrer que les réseaux sociaux étaient plus efficaces pour collecter des données que les modes conventionnels de sondages¹⁰⁹⁹. Du point de vue des données, l'émergence de la sociologie des réseaux complexes et des *data sciences* sur les macro-données est de bon augure pour la recherche scientifique permettant tout à la fois de collecter des données et de faire apparaître des phénomènes nouveaux. Il apparaît que les Relations Internationales ont tous les outils à leur disposition pour profiter des apports de l'informatique dans l'étude de l'information¹¹⁰⁰. Au-delà de

¹⁰⁹⁷ L'auteur fait référence à plusieurs logiciels de lexicométrie et de minage de texte, comme Wordstats, RapidMiner ou encore KHCoder.

¹⁰⁹⁸ Pour un exemple récent, voir : GOEMANS Hein E. et SCHULTZ Kenneth A., « The Politics of Territorial Claims: A Geospatial Approach Applied to Africa, », *International Organization*, vol. 71, no. 1, janvier 2017, pp. 31–64,

¹⁰⁹⁹ RUTHS Derek et PFEFFER Jürgen, « Social media for large studies of behavior. », *Science*, vol. 346, n° 6213, 2014, pp. 1063-1064.

¹¹⁰⁰ Toutefois, malgré des Relations Internationales avec une forte culture pluridisciplinaire, la formation des internationalistes ne va que rarement au-delà des bases en informatique (type C2i).

l’opportunité que ces outils représentent il faut également insister sur l’enjeu politique important que représente l’accès à ces données.

L’enjeu de l’information matérialisée par les données est fondamental pour les sciences humaines et dépasse largement le cadre de la sécurité de l’information. Il dépasse même le cadre de l’opportunité qu’il représente. Le numérique donne lieu à tout un ensemble de pratiques qu’il est nécessaire d’étudier en ce qu’elle impacte non seulement la manière d’étudier les phénomènes politiques mais également les structures de la société. Les enjeux principaux sont liés à la création et l’utilisation des macro-données (ou mégadonnées) dont l’accumulation exponentielle produit un corpus de données impossible à recouper et à analyser pour l’esprit humain¹¹⁰¹. Ces données sont le produit de l’utilisation quotidienne des ordinateurs et des téléphones portables. Sans nous attarder ici sur les volumes gigantesques de données et la prévision de leur croissance du fait de « l’Internet des objets », il y a un vrai défi technique :

« De puissantes ressources informatiques combinées à la disponibilité d’ensembles massifs de données sur les médias sociaux ont donné lieu à un nombre croissant de travaux qui combinent apprentissage automatique, traitement du langage naturel, analyse de réseau et statistiques pour mesurer la structure de la population et le comportement humain à une échelle sans précédent. Cependant, de plus en plus de preuves suggèrent que bon nombre des prévisions et des analyses produites donnent une image fausse du monde réel. »¹¹⁰²

D’un point de vue politique, ces techniques de prévision et d’analyse peuvent permettre de mieux comprendre, voire de résoudre d’importants problèmes sociaux. L’enjeu fondamental de ce type de traitement de données est ainsi prioritairement le ciblage¹¹⁰³. Ce qui change techniquement ici par rapport aux usages précédents de l’outil informatique, c’est le passage des statistiques descriptives sur des données à haute valeur informationnelle aux statistiques inférentielles basées sur des données à faible valeur informationnelle mais avec un grand volume de données. Les applications de tels procédés peuvent concerner non seulement la recherche scientifique, mais également, d’autres domaines d’application comme le secteur

¹¹⁰¹ SHAH Dhavan V., CAPPELLA Joseph N., et NEUMAN W. Russell, « Big data, digital media, and computational social science: Possibilities and perils. », *The ANNALS of the American Academy of Political and Social Science* vol. 659 n°1, 2015, pp. 6-13.

¹¹⁰² RUTHS Derek et PFEFFER Jürgen, 2014, op-cit. p. 1063.

¹¹⁰³ Cela rejoint en partie la culture de renseignement que nous évoquions dans le chapitre 4.

privé, le domaine politique ou dans le secteur de l'énergie. L'ensemble de ces pratiques renvoient traditionnellement à la thématique de la « société en chiffres », à la problématique de la protection des données et en particulier des données personnelles. En ce qu'elle cherche à étudier les processus politiques mettant en jeu notamment des rapports de pouvoir, la Science Politique est toute indiquée pour se saisir de ces problématiques.

Cette thématique appellerait en soit un développement voire un travail de recherche spécifique. Par ailleurs la question de comprendre l'information, faisait actuellement partie des questions les moins développées parmi les travaux relatifs à la sécurité de l'information. Les macro-données sont principalement présentes dans d'autres champs d'étude que celui de la sécurité.

Le langage associé aux concepts, la compréhension de la technologie, de l'agentivité et de l'information sont importants et leurs implications dépassent largement le cadre de cette recherche. Toutefois, chacune d'entre elles représentent une ligne directrice qui aura guidé le choix des théories destinées à répondre plus directement à notre problématique.

Section 2 – Comprendre la sécurité de l'information dans l'étude des Relations Internationales.

Afin de répondre à notre problématique, l'enjeu de la présente section est de déterminer quelles théories répondent le mieux aux quatre grandes questions qui viennent d'être posées à partir des théories évoquées dans le chapitre 4. Un tel exercice d'identification suppose la réduction de ces questions par les résultats de l'analyse de discours.

Cette sélection n'a pas pour vocation de jeter le discrédit sur l'ensemble des théories précédemment évoquées, ni sur le travail d'analyse conduit jusqu'à présent. Par exemple, le concept de sécurisation de l'Ecole de Copenhague s'est avéré utile pour décrire le passage du phénomène linguistique à l'objet de la sécurité de l'information. Néanmoins, c'est ce dernier objet qui nous intéressera ici tout particulièrement.

Il y a deux types d'approches que l'on peut mobiliser pour comprendre la sécurité de l'information dans l'étude des Relations Internationales : des approches globales et des approches centrées sur les cas d'insécurité. Il nous a donc semblé utile de retenir une approche

de chacune de ces catégories. La première approche renvoie aux théories cyberpolitiques de Nazli Choucri formulées entre 1998 et 2019, la seconde approche se concentrera sur l’application de la théorie de l’acteur-réseau au cyber-incident proposée par Thierry Balzacq et Myriam Dunn Cavelty, formulée entre 2012-2016.

A – Les théories « cyberpolitiques » des Relations Internationales.

A ce jour, les travaux de Nazli Choucri représentent sans doute l’un des apports les plus utiles à la compréhension du langage associé au cyberspace et plus largement à la compréhension du rôle de l’information dans les Relations Internationales¹¹⁰⁴. Ces travaux abordent la sécurité, la prise de décision, l’innovation, la gouvernance d’Internet, les câbles sous-marins... Quel que soit l’aspect que ses travaux explorent, on peut toutefois noter trois idées qui ressurgissent le plus souvent : les normes, le contrôle et la durabilité, appuyé par un fort recours aux données quantitatives. Ces travaux semblent pouvoir être inscrit plutôt dans une filiation à l’école américaine de l’économie politique internationale tout en conservant une certaine ouverture.

Dans ces travaux, le cyberspace apparaît comme un élément déterminant et fondamental des Relations Internationales. C’est un phénomène inéluctable doté d’une interconnexion croissante avec la société internationale et qui possède un effet transformateur qui bouleverse la nature des relations entre les acteurs. Ce changement de nature questionne l’applicabilité des théories et des politiques existantes à ce phénomène. En effet, la diffusion accrue des technologies à travers le monde est trop rapide pour être toujours parfaitement prise en compte par un acteur régional qui évolue plus lentement. Il faut ainsi déterminer la bonne adaptation du système international par la mesure des effets provoqués sur cette transformation et réciproquement.

Entre 1998 et 2019, Nazli Choucri a consacré plusieurs publications aux questions liées au cyberspace. Parmi ces publications, nous retiendrons principalement l’article sur les cyberpolitiques publiés en 2000 dans l’*International Political Science Review*, la monographie

¹¹⁰⁴ Théories cyberpolitiques est une appellation sélectionnée dans le cadre de ces développements comme moyen de regrouper l’ensemble des théories mobilisées ici.

publiée en 2012, et l'ouvrage de 2018 coécrit avec David D. Clark¹¹⁰⁵. Cette sélection permettra de mettre en avant trois ensembles de théories centrés autour du domaine politique du cyberspace, et des facultés de ce dernier de transformer les relations internationales.

1 – Les cyberpolitiques et le « *Cyber - IR System* » : le domaine politique du cyberspace.

Reposant sur la définition de 1994 de Benedikt¹¹⁰⁶, la définition du cyberspace retenue dans ces travaux est assez vaste. Il se définit comme une réalité en réseau mondial, qui peut être multi-dimensionnelle, artificielle ou « virtuelle », et qui est assistée par ordinateur, accessible par ordinateur et générée par ordinateur. Cette définition suppose des infrastructures importantes permettant « la mise en place de schémas et de modes d'utilisation gérés par des normes en évolution »¹¹⁰⁷. L'espace est traité comme englobant l'ensemble des domaines d'interaction qui, soutenus par la technologie, sont susceptibles de créer des sources de pouvoir potentiel, fournissant une influence accrue, permettant la création de nouvelles ressources, connaissances ou services. Le cyberspace est donc un contexte construit d'interactions.

Dans ce contexte, en tant qu'allocation de valeur faisant autorité sur la société, une cyberpolitique opère à la rencontre des interactions humaines autour de la détermination de « qui obtient quoi, quand et comment » et de la formation d'espaces virtuels qui assument leurs propres réalités¹¹⁰⁸. Pour comprendre l'étendue de ce domaine politique du cyberspace, il est possible d'employer le concept de « *Cyber - IR system* » qui reprend de manière plus récente

¹¹⁰⁵ Voir CHOUCRI Nazli. « Introduction: CyberPolitics in International Relations. », *International Political Science Review*, vol. 21, no. 3, 2000, pp. 243–263. ; CHOUCRI Nazli, 2012, op-cit. ; et enfin CHOUCRI Nazli et CLARK David D.. *International Relations in the Cyber Age: The Co-Evolution Dilemma*, Cambridge, The MIT Press, 2019, 420 p. Les deux derniers ouvrages font parties d'une série de trois publications sur le thème des interactions entre politiques mondiales et cyberspace. Le troisième n'est pas encore publié.

¹¹⁰⁶ BENEDIKT Michael, 1994, op-cit.

¹¹⁰⁷ CHOUCRI Nazli, 2000, op-cit, p. 244.

¹¹⁰⁸ Cette définition de la cyberpolitique repose sur la combinaison de la définition du cyberspace avec LASSWELL Harold D., *Politics: Who Gets What, When, How*, New York, Meridian Books, 1958, 222 p. ; EASTON David. « An approach to the analysis of political systems. », *World politics*, vol. 9.,n° 3, 1957, pp. 383-400.

ces travaux antérieurs sur les cyberpolitiques. Le « *Cyber-IR system* » un système intégré de couches croisées avec des niveaux d’analyse¹¹⁰⁹.

Le modèle de couches qui est proposé ici est un modèle en quatre couches intégrantes. La première couche est une dimension humaine (*people*) comprenant les individus et leurs regroupements jusqu’aux États. Il s’agit de tous les utilisateurs. Cette couche se caractérise par sa globalité et sa distribution inégale du pouvoir. La deuxième couche est dédiée à l’information qui comprend majoritairement les contenus, ceux-ci étant généralement peu régulés et disponible à bas prix. La troisième couche est une couche de plateforme comprenant des applications (Web, mails.), des services (DNS) et des normes (Internet Protocol). Enfin s’ajoute une couche physique (qui concerne ici prioritairement les machines et les câbles sous-marins) qui représente des investissements forts et est géographiquement localisable. Ce modèle ressemble un peu aux modèles en trois couches (physique, logique, sémantique) auquel il est d’ailleurs fait référence dans des publications antérieures de Nazli Choucri. La plus-value de ce modèle par rapport au modèle en trois couches est qu’il permet une meilleure analyse des activités des acteurs. En effet, là où la typologie physique/logique/sémantique est le plus souvent descriptive et facile d’accès, elle ne parvient pas à démontrer une quelconque efficacité lorsqu’il s’agit d’analyser les modèles de régulation sur des questions précises et n’apporte que peu d’éléments de compréhension des logiques qui prévalent sur cet espace.

La question du niveau d’analyse fait ici appel à des questions plus classiques des Relations Internationales. L’auteure reprend ici les niveaux d’analyse de Kenneth Waltz¹¹¹⁰ : l’individu, l’État et le système international. Trois ajouts sont faits à ce système : le niveau d’analyse global, les organisations à but lucratif et non-lucratif.

« Bien que la création du cyberspace soit le résultat d’activités d’un grand nombre d’individus [...] opérant dans les règles de l’État [...], l’omniprésence et l’utilisation du cyberspace ont une envergure et une portée internationales [...], et la cyberactivité est devenue un élément majeur de l’interaction à tous les niveaux de l’analyse dans les relations internationales. Dans le même temps, toutes les caractéristiques

¹¹⁰⁹ Ce système sera développé dans la première partie de l’ouvrage. CHOUCRI Nazli et CLARK David D., 2019, op-cit. pp 1 – 164.

¹¹¹⁰ WALTZ Kenneth (1959), 2001, op-cit..

habituelles des relations internationales demeurent saillantes ; jusqu'à présent, aucune solution ne semble avoir été remplacée par une alternative au cyberspace »¹¹¹¹

En croisant ces deux grilles de lecture, il est ainsi possible en quelque sorte de cartographier les enjeux de l'information. La cartographie est sans doute perfectible, comme la plupart des organisations thématiques, mais elle a le mérite de livrer toute l'entendue du domaine cyber-politique et de fixer les points où il y a le plus d'enjeux présents¹¹¹². Cette superposition permet de localiser la plupart des acteurs et leurs activités, signaler les changements d'orientations ou de comportement, représenter les activités et ainsi aider à suivre les processus de transformation du domaine cyberpolitique. Par exemple, la couche qui intéresse tous les niveaux d'analyse est l'information. Et il y a plus d'enjeux et de couches concernées par les niveaux d'analyse étatique et des organisations à but lucratif.

Pour rester sur l'exemple de la couche information, les enjeux décrits touchent la vie privée et le travail collaboratif (niveau individuel), la censure (niveau étatique), la protection de la propriété intellectuelle (niveau international), les fuites d'information et le spam (niveau global), les cadres de travail collaboratifs (organisations à but non-lucratif), la collecte des données, le ciblage et la publicité (organisations à but lucratif).

Cette cartographie est assez utile pour commencer à penser à Internet du point de vue politique, néanmoins, elle ne peut permettre d'envisager tous les problèmes de l'information. C'est ici qu'intervient la notion de système complexe. Certains aspects critiques des systèmes complexes ne sont pas facilement représentés par la cartographie et c'est notamment le cas pour les questions de contrôle, de puissance, de sécurité, de gouvernance ou de changement. Autrement dit, il ne faut pas confondre les composants d'un système avec les propriétés émergentes de celui-ci. Une stratégie en couche permet de comprendre le noyau d'un système statique mais pas nécessairement sa manière de fonctionner de façon dynamique.

¹¹¹¹ CHOUCRI Nazli, 2012, op-cit, p. 42.

¹¹¹² Voir CHOUCRI Nazli et CLARK David D., 2019, op-cit. p. 101 - 122.

2 – Les théories de la pression latérale et du réalignement latéral.

Développée à partir de 1972¹¹¹³, la théorie de la pression latérale est une théorie qui vise à articuler la croissance interne d'un État et ses comportements internationaux. Les facteurs internes sont présentés comme étant la cause logique des comportement internationaux des États. Le comportement répond ainsi de variables principales (*master variables*) qui façonnent une identité schématisée par un profil. Ce travail de construction identitaire est favorisé par l'intervention des effets de demandes socialement agrégées et articulées auxquels les comportements internationaux sont destinés à répondre. La pression latérale fait ainsi référence à la propension qu'ont les individus et les sociétés d'étendre leurs activités et exercer une influence et un contrôle au-delà de leurs frontières établies. L'intersection des sphères d'influence de deux acteurs constitue ici le premier pas vers les conflits et la violence.

Cette théorie a été initialement bâtie sur l'ontologie de deux systèmes : l'environnement naturel et le domaine social. Selon la théorie de la pression latérale, chacun de ces systèmes dépend de l'autre. Cette dépendance peut être évaluée du fait que les activités humaines se déroulent dans les deux systèmes. Cependant, la connaissance de la décision est le privilège du domaine social. La nature est ici positionnée dans une logique de boucle de rétroaction (*feedback*). L'apport de l'ouvrage de Nazli Choucri en 2012 est de venir ajouter un troisième système à cette ontologie : Le système « cyber »¹¹¹⁴. Ce n'est pas encore le « *Cyber – IR system* » de 2019 mais il en a déjà de nombreuses caractéristiques.

Dans les théories de la pression latérale, l'individu fournit des efforts afin d'articuler ses demandes et ses besoins avec ceux des autres individus. Cette articulation façonne la société. Celle-ci est moins les résultats de choix conscients et rationnels que d'inertie, d'habitude et de l'adaptation de mélanges d'objectifs personnels et collectifs. L'individu est basiquement représenté comme une entité de traitement de l'information consommatrice d'énergie¹¹¹⁵. Agrégés au niveau sociétal, les individus et leurs demandes les plus fondamentales sont mues par la sécurité et la survie. Les capacités les plus élémentaires souscrivent à ces objectifs. Les

¹¹¹³ CHOUCRI Nazli et NORTH Robert C.. « In Search of Peace Systems: Scandinavia and the Netherlands, 1870-1970, » in RUSSETT Bruce (éd.), *Peace, War, and Numbers*, Berkeley: Sage Publications, 1972, pp 239-274.

¹¹¹⁴ CHOUCRI Nazli, 2012, op-cit.

¹¹¹⁵ NORTH Robert C., *War, Peace, Survival: Global Politics and Conceptual Synthesis*. Westview, 1990, 298 p.

demandes se combinent avec des capacités pour produire des actions. Le résultat de celles-ci dépend des capacités, des connaissances, des compétences et de l'accès aux ressources. La connaissance est au cœur des capacités de l'individu et de l'ordre social. Le cyberespace renforce la diffusion de la connaissance et entraîne des nouveaux besoins dans celle-ci. Il est représenté ici comme un facilitateur de l'expression des individus (notamment dans leurs demandes de sécurité).

Au niveau étatique, la question est plus complexe et dépend essentiellement de l'articulation des variables principales. Trois variables principales sont identifiées par la théorie de la pression latérale : la population (avec ses changements de taille, de distribution et de composition), la technologie (scientifique et institutionnelle) et les ressources (tous les éléments critiques à l'existence). Ces variables entraînent la création de 6 profils type d'États¹¹¹⁶.

Le profil 1 se définit selon l'articulation suivante « **Ressources > Population > Technologie** ». Ces États se définissent selon la disponibilité de ressources potentielles et une contrainte technologique particulièrement forte. L'auteure mentionne ici plusieurs exemples dont l'Angola et le Zimbabwe. De manière générale, ces États sont les moins actifs en termes de cyberpolitique.

Le profil 2 correspond à l'articulation « **Population > Ressources > Technologie** ». Parmi les États de ce profil se trouvent le Maroc ou encore l'Indonésie. Technologiquement limités, ces États ont tendance à être parmi les plus pauvres et les moins développés. Mais bénéficient d'une population importante et d'un accès aux ressources. Certains auront probablement un accès au cyberespace. Ces deux premiers profils soulignent l'importance tautologique de la variable technologique dans l'accès au cyberespace. Encore que, cela n'empêche pas les États cités en exemple d'avoir des politiques de sécurité de l'information.

L'articulation « **Population > Technologie > Ressources** » renvoie vers le profil 3. C'est-à-dire le profil de la Chine, de la Turquie, de la Jamaïque ou de Cuba. Il s'agit d'États qui ont une forte population et des technologies supérieures à leurs ressources. Cela conduit les États à exercer une pression forte à l'extérieur.

¹¹¹⁶ CHOUCHRI Nazli, 2012, op-cit. pp. 32 – 35.

Le profil 4 « **Ressources > Technologie > Population** » de l’Australie ou du Canada désignent de grands États technologiquement avancés avec de fortes ressources. La diffusion et l’usage du cyberespace y est répandue.

Les profils 5 et 6 représentent les États technologiquement les plus avancés. Les États de profil 5 « **Technologie > Ressources > Population** » comme les États-Unis, la Finlande ou la Suède ont un leadership ou une forte participation dans le cyberespace. Le profil 6 « **Technologie > Population > Ressources** » possède une forte population par rapport à ses accès aux ressources et une technologie équivalente au profil 6. Ces États ont également une forte influence dans le cyberespace. S’y trouvent par exemple l’Autriche, le Danemark, la France.

Pour tous ces États quel que soit leur profil, la cybersécurité désigne la capacité de se protéger des menaces qui se réalisent à travers les réseaux. Elle représente la quatrième forme de sécurité après les sécurités interne (liée à la stabilité et à légitimité des institutions), externe (la défense contre les menaces extérieures) et environnementale (habileté de satisfaire les demandes de la population de manière durable). Un État ne possède une sécurité optimale que dans la mesure où toutes les dimensions de la sécurité sont fortes.

La théorie de la pression latérale décrit un certain nombre de transformations sociétales qui entraînent des effets de recomposition dans les structures de la société. Le premier signe de cette recomposition semble être le développement de nouveaux défis à la sécurité nationale, avec de nouvelles sources de vulnérabilité (cybermenaces), de nouvelles dimensions de la sécurité nationale (cybersécurité) et de nouveaux facteurs de peur et d’incertitude. Le deuxième signe de cette recomposition réside dans le développement de nouvelles asymétries et de nouvelles symétries par l’entremise de l’informatique. Corolairement à ce phénomène, il est possible d’observer la montée en puissance de nouveaux acteurs (institutions, entreprises, criminels). Cette prolifération d’acteurs d’envergure internationale est source d’entropie dans le système international. Un autre signe se trouve dans les institutions de « cyber-management » et les querelles qu’elles engendrent qu’il s’agisse d’institutions de gouvernance d’Internet (ICANN) ou pour gérer la sécurité (CERT)¹¹¹⁷. D’un point de vue défense, il faudrait ajouter là cela que la politique de plus en plus interconnectée dans les domaines cinétique et « cyber ».

¹¹¹⁷ Cf. Chapitre 3.

A cela s'ajoutent le cyberconflit, la mise en place des conventions de coopération sur la cybersécurité, la diffusion de l'accès à Internet ou encore le rôle croissant des organisations internationales et le pouvoir d'influence accru des individus. Ce sont autant d'éléments qui indiquent une recomposition. Cette recomposition est qualifiée de réalignement latéral. Le réalignement latéral décrit tout autant le nouveau pouvoir d'influence des individus, que les enjeux de sécurité de l'État, la densité des acteurs parties prenantes de la décision sur la scène internationale ou le développement de la théorie des biens communs au profit d'Internet au niveau global¹¹¹⁸.

3 – Le dilemme de la coévolution et les phénomènes complexes.

Ces phénomènes de transformation invitent à considérer l'impact des phénomènes complexes sur la détermination du futur des Relations Internationales. C'est le rôle d'une autre théorie mise en place à partir de la théorie de la pression latérale, la théorie de la coévolution :

« Nous utilisons les modèles pour mettre en évidence différents scénarios futurs de ce que nous appellerons la co-évolution du cyberspace et des relations internationales - étant donné l'importance croissante de la contention globale dans l'espace partagé. Au cours de nos enquêtes, il est apparu clairement que ces deux domaines, bien qu'apparemment indépendants ou autonomes, devenaient de plus en plus interconnectés de nombreuses manières différentes et inattendues. Cette réalisation a créé un nouveau défi : comment capturer ces interconnexions et comment représenter leurs caractéristiques. La nouvelle « réalité » est que nous avons maintenant affaire à un système extrêmement complexe. »¹¹¹⁹

La coévolution désigne l'influence réciproque du cyberspace et des relations internationales entendues au sens des théories et des politiques, mais aussi des pratiques. La politisation croissante du cyberspace et ses implications pour les relations internationales engendrent ce que les auteurs désignent ici sous l'expression de « dilemme de la coévolution ». Ce dilemme repose sur une incapacité des deux ensembles à évoluer de manière homogène et uniforme. Les éléments qui constituent chacun des domaines évoluent tous à des rythmes différents ce qui engendre de l'imprévisibilité et des incertitudes. Le « *Cyber - IR System* » y constitue l'une des réponses.

¹¹¹⁸ Sur ce dernier point, voir chapitre 4

¹¹¹⁹ CHOUCHRI Nazli et NORTH Robert C., 2019, op-cit, p. viii.

Le système international est actuellement construit dans une conception de l'autorité basée sur l'État. Le cyberespace repose presque entièrement sur le pouvoir et la pratique de l'autorité privée. L'importance du secteur privé est incompatible avec le rôle qui lui est attribué dans la théorie traditionnelle des relations internationales. C'est l'un des premiers phénomènes complexes à saisir. Sauf exception, l'État dans sa globalité n'exerce qu'une souveraineté limitée sur le cyberespace par la législation et la réglementation, les achats, les investissements en recherche et développement, la participation au processus de normalisation et les actions plus diffuses. L'État n'exerce sa souveraineté que de manière « déléguée » en passant par des personnes privées intermédiaires qui contrôlent et façonnent directement Internet¹¹²⁰.

La complexité réside principalement dans le dépassement de la perception des acteurs. Cela rejoint des éléments que nous avons relevé au cours de cette recherche. Classiquement en matière de sécurité, les acteurs sont définis, les actions observables et souvent mesurables en termes de type, d'intensité de l'hostilité et d'impact. Ce n'est pas le cas dans le cyberespace. L'identité des acteurs doit y franchir l'étape de l'attribution. Les attaques demandent des ressources particulières pour être observables et elles sont difficiles à évaluer en termes d'impact. Les auteurs opèrent l'étude de 17 cas de piratage informatique et d'attaques informatiques afin d'en déterminer les traits caractéristiques¹¹²¹. Il apparaît ainsi qu'une cyberattaque s'inscrit le plus souvent dans la suite d'un conflit « physique » et qu'elle n'a pas une alternative mais un complément aux modes d'action conventionnel. Seulement un tiers de ces attaques avait une portée globale. L'impact d'une cyberattaque semble augmenter lorsqu'elle est commanditée ou aidée par des moyens étatiques. Quasiment toutes les attaques ont une cible ou un initiateur qui est une personne privée. Les cibles varient énormément d'un cas à l'autre. Parmi les personnes privées, certains individus ont une plus grande participation dans les cyberconflits que dans les autres formes de conflits. Le type d'attaque le plus répandu est l'attaque par déni de service. La sophistication des logiciels malveillants payants n'a cessé d'augmenter avec un pic en 2013.

Ainsi les théories « cyberpolitiques » décrivent une vision holiste du cyberespace et de sa transformation des Relations Internationales. L'interdépendance mise en avant entre

¹¹²⁰ Les auteurs développent une méthode d'analyse basée sur les « points de contrôle » pour mettre en valeur cette réparation du pouvoir.

¹¹²¹ CHOUCHRI Nazli et NORTH Robert C., 2019, op-cit, pp. 209 - 246.

Relations Internationales et cyberespace pourrait viser un certain déterminisme néanmoins les scénarios proposés et la pluralité des profils d'État contredisent cette assertion.

B – Vers une casuistique de la cybersécurité : l'apport de la théorie de l'acteur-réseau.

Après avoir abordé une vision holiste du cyberespace et de son impact sur les Relations Internationales, nous allons aborder un autre point de vue centrée sur une étude de cas à travers la théorie de l'acteur-réseau. L'avantage ici est double : répondre à la question du déterminisme technique, et dépasser le niveau strictement normatif pour envisager une étude de cas concrète, ce que les théories « cyberpolitiques » ne permettent pas de faire directement. L'un des principaux atouts de la théorie de l'acteur-réseau est que grâce aux concepts développés (actant, traducteur, médiateur), les technologies ne sont pas de simple contingence mais au contraire des éléments actifs influençant positivement ou négativement la sécurité. Autrement dit, la technologie n'est plus déterminée dans un rôle de médium mais joue un rôle direct dans l'évènement objet de l'analyse.

Peu d'auteurs ont tenté d'appliquer la théorie de l'acteur-réseau à la cybersécurité et lui préfèrent souvent d'autres concepts comme la gouvernance polycentrique¹¹²². Parmi les auteurs ayant travaillé sur la cybersécurité, la tentative la plus aboutie d'appliquer la théorie de l'acteur-réseau à la cybersécurité est l'analyse de Stuxnet de Thierry Balzacq et Myriam Dunn Cavelty¹¹²³. Par l'analyse de Stuxnet, cette étude a pour objectif de théoriser la cybersécurité d'après la théorie de l'acteur-réseau. Il existe bien évidemment d'autres tentatives plus anciennes, mais la plupart ne concernent pas directement la cybersécurité au sens strict ou sont trop spécifiques¹¹²⁴. L'article de Thierry Balzacq et Myriam Dunn Cavelty servira ainsi de référence pour cette casuistique de la cybersécurité.

¹¹²² Sur les cyberattaques, SHACKELFORD Scott J., 2013, op-cit. ; Sur le cybercrime, DUPONT Benoît, 2016, op-cit.

¹¹²³ BALZACQ Thierry et DUNN CAVELTY Myriam, « A theory of actor-network for cyber-security », *European Journal of International Security*, Vol. 1, part 2, 2016, pp. 176–198. ; voir également DUNN CAVELTY Myriam, 2018, op-cit.

¹¹²⁴ Pour une synthèse des études, voir STEVENS Tim. « Global Cybersecurity: New Directions in Theory and Methods. », 2018,. Voir sur la contrefaçon de musiques : HINDUJA Sameer. « The Heterogeneous Engineering of

1 – Le concept de « cyber-incident ».

Le cas sélectionné par les auteurs est celui du ver informatique Stuxnet découvert en 2010 qui a défrayé la chronique et lancé le second débat sur les « cyberarmes » en France¹¹²⁵. C'était un ver d'une grande complexité ayant nécessité probablement plusieurs années de développement et conçu pour cibler des systèmes spécifiques et s'infiltrer dans certains automates industriels. Le ver est connu pour avoir ciblé l'Iran en particulier ses centrales nucléaires, mais il a affecté de nombreuses machines dans d'autres États en particulier en Inde¹¹²⁶. Stuxnet est décrit comme un « cyber-incident ».

Dans le cadre de cet article, un cyber-incident est une perturbation délibérée des pratiques de cybersécurité normalisées par un logiciel malveillant, ayant des effets politiques différents sur l'imagination et les interventions¹¹²⁷. La notion d'incident est ici définie plus strictement que ce que couvre la notion habituelle d'incident. Le logiciel est décrit comme un artefact du langage implémenté physiquement. Ce logiciel existe par les effets qu'il produit, et ces effets sont ceux qu'il énonce. Cela permet aux auteurs de décrire le logiciel comme une forme de performance¹¹²⁸. Dans la plupart des cas, le logiciel malveillant est l'élément déclencheur du cyber-incident. La plupart des réponses au cyber-incident sont donc des réactions.

Afin de compléter ce modèle du cyber-incident, il fallait conceptualiser l'agentivité des non-humain (le logiciel), le phénomène de perturbation (réalisation du cyber-incident) et les relations entre objet et espace. Thierry Balzacq et Myriam Dunn Cavelty ont décidé d'avoir recours à la théorie de l'acteur et en particulier à trois concepts : l'actant, la dé/ponctualisation et la performance des espaces. Ayant déjà défini l'actant¹¹²⁹, nous allons nous attarder sur les deux autres concepts. Signalons juste que les auteurs choisissent ici le « médiateur » qui permet

Music Piracy: Applying Actor-Network Theory to Internet-Based Wrongdoing. » *Policy & Internet*, vol. 4, n° 3-4, 2012, pp. 229–248. ;

¹¹²⁵ Cf. chapitre 1 pour un commentaire sur la notion de cyberarme.

¹¹²⁶ DE FALCO Marco, 2012, op-cit.

¹¹²⁷ BALZACQ Thierry et DUNN CAVELTY Myriam , 2016, op-cit. p. 181

¹¹²⁸ Sur la performativité des énoncés, cf. Chapitre liminaire. Le logiciel est ainsi défini par son code comme un acte du langage ayant des effets politiques. Son caractère malveillant reçoit une lecture téléologique de son utilisation (caractère délibéré), mais ne se déduit pas seulement de sa conception.

¹¹²⁹ Cf. chapitre 4.

de distinguer l'agentivité du cyber-incident de celle de l'assaillant, et définir le potentiel destructeur du virus comme étant toujours actif.

La ponctualisation est un effet d'encapsulation qui décrit l'ensemble des actants d'un système complexe comme agissant comme un seul actant. Autrement dit lorsque le réseau n'est plus qu'un point et que chacun des actants devient indissociable. La ponctualisation est l'objectif de la cybersécurité. Cet objectif est contredit par le cyber-incident qui opère une « déponctualisation ». Les parties défaillantes du système attaqué redeviennent théoriquement visibles.

La performance des espaces¹¹³⁰ est un concept qui renvoie à la création des espaces du fait de la performance des objets, qui sont considérés comme des actants.

« En d'autres termes, tous les rapports sociaux sont des assemblages complexes d'entités sociotechniques et tout phénomène tire sa forme et son contenu du réseau de relations auquel il participe. »¹¹³¹

Ce concept implique que le cyber-incident doit être examiné dans son propre espace¹¹³². Faisant la somme de ces concepts les auteurs décrivent finalement le cyber-incident comme des « déponctualisations de réseaux de cybersécurité par des médiateurs se présentant sous la forme de logiciels malveillants, avec des effets dans les espaces régionaux, en réseau et fluides »¹¹³³.

2 – Application de la théorie de l'acteur-réseau : topologie et sécurité.

A partir de cette seconde version de leur concept, les auteurs présentent un modèle de sécurité basé sur une topologie composée de trois types d'espaces interconnectés entre eux : Les espaces régionaux, en réseau et fluides. Ces trois espaces sont composés par les actants et les relations qu'ils entretiennent entre eux par la création de leurs espaces respectifs. La sécurité

¹¹³⁰ LAW John, « Objects and Spaces. » *Theory, Culture & Society*, vol. 19, n°. 5–6, 2002, pp. 91–105

¹¹³¹ BALZACQ Thierry et DUNN CAVELTY Myriam , 2016, op-cit. p. 184 (Notre traduction)

¹¹³² Nous laissons ici de côté les développements relatifs au cyberspace à sa nature pour nous concentrer sur l'appréhension du cyber-incident.

¹¹³³ Ibid. p.185. Les trois types d'espaces font référence à l'article : MOL Annemarie et LAW John « Regions, networks and fluids: anaemia and social topology. » *Social studies of science*, vol. 24, n°4, 1994, pp. 641-671.

est une pratique sociopolitique est « négociée à l'intérieur et entre les trois espaces », chacun « activant différents types d'opérations »¹¹³⁴.

Si l'on devait résumer la teneur particulière de chacun de ces espaces, la région est ce qui ressemblerait le plus à un État au sens classique du terme (même si elle ne se limite pas à cette seule espèce). Elle est définie par des frontières claires et un tout cohérent. Il y a un intérieur et extérieur à la région. Par opposition le réseau n'est pas constitué par sa position dans l'espace, celle-ci existe mais n'est pas déterminante de sa nature. Le réseau contredit le phénomène hiérarchique par une forme d'horizontalité. Toutefois, la région et le réseau fonctionnent d'une manière semblable du point de vue de la sécurité, chacun de ses espaces recherche la sécurisation de ses points de vulnérabilité aux fins d'assurer sa continuité (donc la conservation relative de la forme de son espace). La fluidité représente l'échec de cette sécurité. On retrouve dans ce système des traces du modèle de description du cyberespace en trois couches (physique/logique/sémantique). La région pouvant revendiquer la couche physique, le réseau la couche logique et les objets la couche sémantique.

La région représente ainsi le domaine d'appréhension du cyber-incident. Elle comprend toutes les machines et toutes leurs infrastructures où la déponctualisation s'opère. La région représente également la première ligne de construction d'une cybersécurité efficace. Les réseaux représentent à la fois un domaine d'infection, un domaine de lutte et un domaine de normalisation de la sécurité de l'information. Ils apparaissent ainsi comme une forme d'interface. Enfin de son côté l'espace fluide manifeste l'incertitude par le biais du logiciel malveillant. Cet espace représente l'incertitude entre le moment de la déponctualisation, sa perception et l'identification du caractère malveillant du logiciel concerné (qui fait rebasculer l'espace dans sa forme de réseau). Ce rapport à l'ordre et au désordre interroge tout particulièrement la nature de l'information. La logique de fonctionnement décrite ici pourrait également constituer l'une des raisons pour lesquelles le cyberespace jouit d'une représentation particulièrement négative et pourquoi le phénomène du langage ne recoupe presque plus que des termes orientés vers la sécurité.

Il est relativement intéressant de comprendre cette typologie et son fonctionnement par l'étude de Stuxnet. La déponctualisation de Stuxnet commence à partir du moment de sa

¹¹³⁴ Ibid. p. 191.

découverte en juin 2010 jusqu'à son identification en juillet 2010. D'après l'étude, l'espace fluide a plusieurs effets en termes de technique et d'attribution. Cela engendre une forme d'incertitude sur l'identité et les capacités de l'ennemi. Ainsi la menace technique devient une menace politique par le biais de la fluidité de l'espace. Cette incertitude outre le besoin de sécurité engendre également une recherche de vérité¹¹³⁵. Cet espace fluide parvient ainsi à décrire chacun des aspects de la cybermenace. Ici la sécurité passe par la connaissance.

3 – Le langage « cyber » comme réponse à l'ignorance.

Cette étude est particulièrement intéressante dans la mesure où le cadre théorique proposé dépasse la seule question de la cybersécurité. En présentant celle-ci comme la construction d'une connaissance pratique humaine et non-humaine, cette théorie interroge à la fois l'extension possible à d'autres objets techniques mais également le rôle du discours savant qui vient structure cet enjeu de sécurité.

Du point de vue du langage, cette théorie nous semble un complément utile à l'analyse de discours (fiction instituante, logométrie, communauté épistémique, sécurisation) en ce qu'elle apparaît justifiée la manière dont le phénomène linguistique évolue, une partie de la métaphore du cyberspace et de la communauté discursive qui s'est construite autour de lui. Par ailleurs, elle vient expliquer les tendances du discours à l'exagération ainsi qu'un peu du fétichisme de la technique. Le point de vue de l'articulation entre l'ordre et le chaos renvoie quant à lui à la place occupée quotidiennement par la cybersécurité comme une forme de rites : identifications par mot de passe, renouvellement de ceux-ci, autocontrôle des correspondances écrites, la permanence de l'antivirus. Autant d'élément qui participer à réduire l'espace fluide. Là où l'anonymat, les logiciels malveillants, l'opacité sont autant de variable qui entretiennent l'espace fluide.

Pour établir un lien avec la théorie de la coévolution, l'absence de connaissance sur la forme qu'auront demain la région et le réseau du fait du pouvoir transformateur de leur interaction réciproque (coévolution) et asymétrique (le réseau évolue plus vite que la région), engendre également une forme de fluidité dans l'évolution de la région qui caractérise le

¹¹³⁵ Ibid. p. 195.

« pouvoir transformateur du cyberspace ». L’assistance sur le rôle clef de l’acteur régional et l’hypersécurisation apparaîtrait alors comme une conséquence de la présence de cette fluidité.

Conclusions de chapitre.

Ce dernier chapitre avait pour fonction de réaliser la combinaison pragmatique conduite par les problèmes à partir des réceptions de la sécurité de l’information dans les Relations Internationales. Ceci nous avait permis de dégager quatre questions :

1. Les Relations Internationales doivent-elles employer le langage « cyber » pour formuler leurs concepts ?
2. Quelles approches peuvent être utiles aux Relations Internationales pour étudier les artefacts technologiques sans tomber dans le déterminisme ?
3. Comment la sécurité de l’information impacte-t-elle l’agentivité en Relations Internationales ?
4. Est-il possible d’utiliser l’information comme un objet d’étude pour comprendre la dimension internationale du politique ?

Chacune de ces questions appelaient plusieurs réponses possibles. Au sujet du langage, la principale conclusion était que ce n’était tant un problème du langage en lui-même que de la fonction englobante et fédératrice qui était la sienne. En tant que notion, le cyberspace semble encore utile à la valorisation des résultats de la recherche, et rien n’interdit aux chercheurs d’en faire des concepts.

La question de la technologie était plus complexe. Il en ressort principalement que les Relations Internationales peuvent développer des approches intéressantes pour travailler sur la technique à condition de mobiliser des théories issues de la sociologie des sciences et techniques. Sur la base des travaux de l’ouvrage collectif de Daniel McCarthy, quatre théories ont semblé utiles : la théorie critique des technologies, la construction sociale des technologies, les nouveaux matérialismes et la théorie de l’acteur-réseau.

L’agentivité s’est vue opposer des contraintes fortes concernant les acteurs à prendre en compte ainsi que dans les rapports de pouvoir (asymétrie) qu’ils exerçaient entre eux. L’impact

de la sécurité de l'information sur les Relations Internationales conduit ainsi à privilégier les théories les plus ouvertes possibles.

Enfin, l'information était paradoxalement la question la moins présente dans les théories analysées. La prise en compte de l'information comme objet par l'usage des outils informatiques semble possible dans le cadre des Relations Internationales computationnelles, bien que cela nécessite passer un certain stade de développer des compétences spécifiques sans doute hors de la portée de la plupart des internationalistes du fait des formations actuelles.

D'une manière générale, chacune des théories évoquées dans ce chapitre que ce soit en première ou seconde section offre une vision plus large que la seule transformation de l'information en objet de sécurité. L'étude de cette transformation, et cela répond aussi en partie à notre problématique, renvoie les Relations Internationales à des questions fondamentales qui ne sont pas sans rappeler les grands débats inter-paradigmatiques tout particulièrement lorsqu'il s'agit d'évoquer la possibilité du recours à des méthodes quantitatives renouvelées et des questions qui impactent profondément la définition de l'acteur.

La seconde section de ce chapitre nous aura permis d'aborder deux ensembles théoriques destiné à fournir une explication au phénomène de la sécurité de l'information dans les Relations Internationales : les théories « cyberpolitiques » formulées par Nazli Choucri avec l'aide d'autres chercheurs du MIT et la théorie de l'acteur-réseau appliquée à la cybersécurité par Thierry Balzacq et Myriam Dunn Cavelty. Le premier ensemble théorique principalement issu de l'économie politique internationale offre grâce au concept de domaine cyberpolitique un panorama presque complet des enjeux de l'information. Le second ensemble théorique centré sur l'acteur-réseau mobilise les concepts de performance et de l'acteur-réseau pour fournir une lecture dynamique de l'étude du fonctionnement des cyber-incident et de leur impact politique. L'ensemble des cadres théoriques développés éclairent les enjeux normatifs, techniques et politiques de la sécurité de l'information.

Vis-à-vis de la transformation de l'information en enjeu de sécurité, l'approche des cyberpolitiques permet principalement d'en mesurer la diffusion à la fois par la cartographie des enjeux dans le cadre du « *Cyber-IR system* », mais également dans la théorie de la pression latérale grâce aux profils des États. L'approche de l'acteur-réseau dresse un portrait abstrait de

la cybermanace au travers de l'espace fluide qui illustre les ressorts du discours « cyber » dans ses phénomènes d'hypersécurisation et de pratiques quotidiennes.

La combinaison des deux théories peut s'établir à l'aune de la perception. Dans les deux ensembles théoriques, la complexité réside principalement dans le dépassement de la perception des acteurs. Dès lors, le fait de pouvoir retrouver la maîtrise de l'artefact technologique par le biais de la connaissance sera l'une des solutions mise en œuvre dans les deux ensembles. Ce qui leur permet de souligner les aspects de technification de la sécurité de l'information.

En cela, mises en parallèle avec le discours, ces deux théories apparaissent complémentaires avec la fiction instituante de Lucien Sfez (Chapitre 1), la communauté épistémique centrée sur le discours (chapitre 3) et avec les grammaires de la cybersécurité sans l'idée de système autonome (chapitre 4). Un texte explicatif idéal devra être rédigé de façon inclure ces théories-là également.

Conclusion générale.

Il s'agit tout d'abord dans cette conclusion de revenir sur les grandes lignes de la démarche de recherche proposée par cette étude. Cela sera suivi de la formulation de la réponse à la problématique. Enfin, cette partie se terminera par des pistes de réflexion sur l'information dans les Relations Internationales.

Retour sur la démarche de recherche.

Entamée sur un questionnement relatif à l'éventuelle nature d'objet du cyberespace dans les Relations Internationales, cette recherche a adopté une problématique double : Comment les Théories des Relations Internationales peuvent-elles comprendre le cyberespace ? Que peut apporter le cyberespace à la compréhension et à l'étude des Relations Internationales ?

Cette problématique impliquait se demander ce qu'était le cyberespace mais aussi de se demander comment comprendre le langage formé de l'ensemble des mots dérivés qui lui étaient apparentés par le préfixe « cyber- ». En outre, il fallait s'interroger sur le sens de ce phénomène en termes de représentations et de modèles théoriques associés.

L'hypothèse principale de cette recherche a été construite autour du postulat que le cyberespace et ses termes dérivés participaient d'un même phénomène discursif. L'objet de travail principal de cette thèse résidait dans l'étude de ce phénomène du langage. La réponse à la problématique impliquait ainsi un échange entre les modèles théoriques des Relations Internationales et le cyberespace compris comme phénomène du langage. Ici est apparue la première difficulté. D'un côté, le phénomène du langage était animé par une actualité particulièrement intense riche en variations de forme et de sens. De l'autre côté, les Relations Internationales étaient grevées par de nombreux paradigmes *a priori* incommensurables. Cette situation un peu complexe était renforcée par le fait que le milieu de la recherche française était balbutiant sur la question du cyberespace et qu'il n'y a eu pas encore de programme de recherche spécifique en France. Par ailleurs, à quelques exceptions près, la majorité de la production française à caractère scientifique sur le sujet était plutôt dédiée à la vulgarisation.

Afin de dépasser cet obstacle, la thèse a été peu à peu réorientée vers l'idée d'un modèle épistémologique croisant une approche sociologique centrée sur le discours avec une approche éclectique des Relations Internationales liées entre elles par une logique abductive. Pour la sociologie du discours, c'est le concept d'espace sémantique de Jean-Claude Passeron qui a finalement été retenu afin de faire le lien entre le langage dit naturel et le langage logique. Début 2013, la découverte de la thèse de Jérémie Cornut et du pragmatisme conduit par les problèmes a fourni l'autre pilier de l'épistémologie de cette thèse.

Sur le plan méthodologique, l'important travail théorique ainsi que le recours à une approche quantitative et qualitative (logométrie), combinée avec des approches exploratoires du terrain (principalement l'observation participante), ont permis de récolter de nombreuses données utiles.

L'architecture du manuscrit reflète en grande partie cette construction intellectuelle. La première partie est dédiée à la collecte de données et à l'analyse de discours. Celle-ci opère à partir du croisement de plusieurs approches méthodologiques dans une phénoménologie plurale destinée à déconstruire le phénomène linguistique « cyber » comprenant la notion de cyberspace (Chapitre 1), les termes dérivés (Chapitre 2) et la communauté associée (Chapitre 3). La seconde partie du manuscrit est quant à elle dédiée à la combinaison pragmatique. Cette combinaison opère en plusieurs temps. Tout d'abord, il y a la traduction du phénomène du langage dans les Relations Internationales et la question de ses réceptions (Chapitre 4). Et enfin, la formulation des questions théoriques et des théories des Relations Internationales qui peuvent y répondre (Chapitre 5). Le tout est précédé d'un chapitre liminaire destiné à exposer le cadre retenu pour cette recherche.

Ce dernier aborde en premier lieu la question des Théories des Relations Internationales permettant de mettre en avant l'option pour le pragmatisme conduit par les problèmes. Il traite dans un deuxième temps de l'analyse de discours en établissant des liens avec les études de sécurité et l'épistémologie de Jean-Claude Passeron. Après avoir présenté l'approche plurale du phénomène du langage et l'apport de la démarche abductive, ce chapitre finit par évoquer l'engagement comme officier sous contrat dans l'armée de l'Air ayant eu lieu en cours de thèse en 2014 et l'évolution des principales contraintes matérielles et scientifiques auxquelles la thèse aura dû faire face.

Afin de répondre à la problématique, la thèse mobilise la démonstration suivante.

Le premier chapitre de la thèse se concentre sur la définition de la notion de cyberespace au regard de son rapport à la technique et de son pouvoir évocateur. Le chapitre évoque la création, les héritages et les confusions autour du cyberespace. Puis, il se concentre sur l'impossibilité d'en donner une définition technique satisfaisante.

Le deuxième chapitre est dédié à l'analyse logométrique des contextes d'emploi des termes dérivés du cyberespace entre 2001 et 2016 dans cinq corpus. Sur la période considérée, les corpus sont constitués de toutes publications en français contenant des termes composés du préfixe « cyber » :

- dans le Journal Officiel de la République française (corpus 1),
- dans le Journal Officiel de l'Union Européenne (corpus 2),
- dans le système de diffusion électronique des documents de l'ONU (corpus 3),
- dans les articles de presse de la plateforme Factiva (Corpus 4),
- dans les articles de presse de la plateforme Google News (Corpus 5).

Ce deuxième chapitre se termine sur une première analyse des résultats.

Le troisième chapitre est dédiée à l'analyse de la communauté à caractère scientifique associée au phénomène linguistique dans lequel converge la sécurité de l'information, le langage « cyber » et les intérêts étatiques. Ce chapitre opère une relecture de la communauté épistémique par la communauté discursive, une étude des « frontières » de la communauté au niveau politique, technique et par le discours. Le chapitre termine par une plus longue étude du phénomène linguistique en France au travers de l'influence américaine, de l'émergence de la sécurité informatique comme enjeux public, de sa transformation en enjeu de sécurité nationale et enfin du rôle de la recherche dans ce processus.

Dans la seconde partie de cette thèse, le quatrième chapitre relève des éléments du discours précédemment identifiés, pour les confronter à la théorie de la sécurisation de l'Ecole de Copenhague. Puis il envisage l'ouverture de ce cadre par l'inscription du phénomène du cyberespace dans un ensemble plus large (la sécurité de l'information) dont il analyse ensuite la réception dans les Théories des Relations Internationales.

Le cinquième et dernier chapitre, plus court, opère la synthèse des questions majeures posées par la réception de la sécurité de l'information dans les Relations Internationales. Quatre questions ont été identifiée : l'utilisation du langage « cyber », l'étude des technologies, l'impact sur l'agentivité et enfin l'étude des Relations Internationales par l'information. Après avoir exposé différentes pistes pour répondre à chacune de ces questions, le chapitre propose deux ensembles théoriques pour résoudre la plupart de ces questions : les théories cyberpolitiques de Nazli Choucri, et la cybersécurité sous le prisme de la théorie de l'acteur-réseau par Thierry Balzacq et Myriam Dunn Cavelty.

Entre discours et sécurité de l'information, comprendre le cyberespace dans les Relations Internationales.

En réponse à la problématique de cette recherche, il est possible de décrire le cyberespace comme une fiction technopolitique (Chapitre 1) qui alimente un phénomène du langage composé de nombreux termes dérivés employés majoritairement pour décrire des enjeux de sécurité (Chapitre 2). La sécurité de l'information est légitimée et diffusée par une communauté épistémique (Chapitre 3). Le cyberespace est donc un discours de sécurité dédié à l'information et pouvant être compris par les théories de la sécurisation. Toutefois, l'enjeu de la sécurité de l'information dépasse de loin le seul langage « cyber » (Chapitre 4). Les questions engendrées par la réception de la sécurité de l'information et les théories sélectionnées peuvent être regardées comme un apport du cyberespace à la compréhension des Relations Internationales (Chapitre 5).

Ainsi les principales théories et concepts qui éclairent la compréhension mutuelle du cyberespace et des Relations Internationales peuvent être résumés ainsi. Reprenant une partie des conclusions antérieures, chacun de ces éléments forme une partie du texte explicatif idéal du phénomène complexe étudié.

1 – Le cyberespace, une fiction technopolitique (Lucien Sfez).

Né de la science-fiction des années 80, le cyberespace opère dans la description métaphorique d'un espace fictif centré sur les représentations abstraites des objets techniques qui forment autant de fétiches pour alimenter un discours où la sécurité incarne une réponse

pratique à une information qui dans le discours s'affranchit apparemment de toute maîtrise. En tant que fiction technopolitique, le pouvoir évocateur du cyberspace procède d'une structure fictionnelle constituée par une représentation spatiale simplifiée et totalisante de l'information. L'arlesienne de la définition technique ou scientifique d'un cyberspace qui se dérobe apparaît comme impossible à résoudre. Le cyberspace est créé dans la littérature à partir d'un fond commun scientifique et culturel qui emprunte beaucoup au champ de la recherche scientifique. Son sens est ensuite déformé et réapproprié pour donner lieu à une appropriation globale des technologies de l'information, d'Internet, des médias et de la robotique. Cette appropriation fait naître des fétiches du discours composés de personnages conceptuels et d'artefact répétés.

Ici, le cyberspace est une fiction technopolitique en ce sens qu'il est d'abord un discours sur une certaine technique.

2 – Le cyberspace, un phénomène du langage (Jean-Claude Passeron, Max Reinert).

En tant que phénomène du langage, les analyses logométriques démontrent que le cyberspace apparaît comme un phénomène croissant tout du long de la période analysée (2001-2016) quel que soit le corpus. Le cyberspace est un terme qui connaît de nombreuses variations de formes *ad hoc* qui ne trouvent leur sens que dans le rapport au contexte et au matériel employé qui les constituent spécifiquement. Ces formes nouvelles éclipsent presque totalement le cyberspace de la littérature analysée.

Les discours analysés mettent en avant une position clef de l'acteur régional ; là où l'individu semble apparaître à la marge dans les niveaux locaux et internationaux. L'État est l'acteur principal pour lutter contre les menaces liées à la sécurité de l'information y compris au niveau de l'ONU.

Les principaux déterminants ou enjeux du contexte d'emploi des cybromots sont : menace, protection, sécurité, criminalité, défense. Ils sont rejoints par une série de thématiques secondaires : gouvernance, gestion des flux de données, résilience.

Dire que le cyberspace est un phénomène du langage revient à mettre l'accent sur ses nombreuses mutations.

3 – Le cyberespace, un discours dans la communauté de la sécurité de l’information (Mai'a Cross, Claudio Radaelli).

« Être un membre de la communauté épistémique de la sécurité de l’information, c’est être quelqu’un avec qui il est possible d’en parler » affirmait le chapitre 3. Cette aptitude à la controverse repose sur la maîtrise du discours. En utilisant le concept de communauté épistémique centré sur le discours, le chapitre a mis en lumière des phénomènes d’influences qui pouvaient exister dans celui-ci. La communauté désigne le phénomène dynamique de redistribution des rapports de force dans l’espace sémantique relatif à un enjeu de la sécurité de l’information. La définition de la perception d’un problème et la controverse qu’elle implique forment les limites de l’espace sémantique où la communauté peut hiérarchiser ses membres. Cette hiérarchie communautaire existe en complément de la hiérarchie propre de chacun des acteurs. Cette communauté particulière de la sécurité de l’information en France se développe autour des discours et notamment le discours qui allie la sécurité de l’information au langage « cyber » comme un intérêt de l’État. Ce discours se développe à l’étranger notamment aux États-Unis dans les années 90, et commence à émerger durant la même période en France à quelques années de différence. Sa consécration est effective en France en 2008 et c’est seulement alors que la communauté épistémique centrée sur le discours peut se développer. Il est en effet important de souligner que c’est bien une impulsion de l’acteur régional qui décide de consacrer cet enjeu par ce langage particulier qui entame le développement de l’intérêt des autres acteurs utilisant le même langage. L’influence américaine dans la communauté est notamment marquée par la création de concept : cyberespace, cyberguerre, le modèles des « couches » mais aussi par un travail d’influence des normes comme l’indique la controverse autour de l’élaboration des *Manuels de Talinn*.

Ici le cyberespace existe avant tout comme un discours labellisant l’activité de certains acteurs pour en faire des membres de la communauté.

4 – Le cyberespace, un discours de sécurité (Lene Hansen, Helen Nissenbaum, Mary Manjikian, Nazli Choucri).

Avec le discours comme point de départ, la théorie de la sécurisation de Nissenbaum et Hansen a permis de traduire le langage en opérateur de conversion de l’information en enjeu

de sécurité. Cet opérateur de conversion illustrait par les grammaires qu'il mobilisait l'exagération (hypersécurisation), les pratiques quotidiennes et le rôle particulier des experts (technification).

Nous retiendrons ici l'apport de Mary Manjikian qui propose de différencier trois grandes postures pour conceptualiser le cyberespace : utopique (*utopian*), réglementaire (*regulatory*) et réaliste (*realist*). Chacune de ces postures renvoie à des conceptions différentes du territoire, du pouvoir, de l'identité, de la crédibilité de l'acteur régaliens, de l'information, de régulation et de la croissance de celle-ci. Ces développements ont permis de mettre en avant une certaine forme de déterminisme technologique présent dans les Relations Internationales depuis leurs origines, un impact non négligeable des paradigmes sur l'apprehension de la sécurité de l'information, et enfin, une place importante des récits dans le traitement scientifique de ces enjeux. L'analyse d'un échantillon des thématiques des publications a démontré que la majorité des publications sur la cybersécurité restent axées sur les politiques publiques et la résolution de problèmes avec pour la plupart d'entre elles, un rapport relativement distant à l'empirie. De fait, la technologie apparaît comme une thématique traitée de manière insuffisante dans les Théories des Relations Internationales.

Le cyberespace est avant tout compris ici en tant qu'opérateur de conversion qui transforme l'information en enjeux de sécurité.

5 – Le cyberespace, un mode d'interactions mult;niveaux dans les Relations Internationales (Nazli Choucri).

Comprenant le « Cyber-IR system », et les théories de la pression latérale et de la coévolution, les théories « cyberpolitiques » de Nazli Choucri présentent le cyberespace comme un contexte construit d'interactions. Le système « cyber » devient ainsi le troisième mode d'interaction dans la théorie de la pression latérale après le domaine social et l'environnement naturel. Dans ce contexte, en tant qu'allocation de valeur faisant autorité sur la société, une cyberpolitique opère à la rencontre des interactions humaines autour de la détermination de « qui obtient quoi, quand et comment » et de la formation d'espaces virtuels qui assument leurs propres réalités.

Le cyberespace interagit à tous les niveaux, de l'individu jusqu'au niveau du système international, créant une forme d'interdépendance complexe entre l'évolution des Relations Internationales et la sienne (Coévolution). La politisation croissante du cyberespace et ses implications pour les relations internationales engendrent ce que les auteurs désignent ici sous l'expression de « dilemme de la coévolution ». Ce dilemme repose sur une incapacité des deux ensembles à évoluer de manière homogène et uniforme. Les éléments qui constituent chacun des domaines évoluent tous à des rythmes différents ce qui engendre de l'imprévisibilité et des incertitudes et impliquant le développement de politiques de sécurité spécifiques.

Le cyberespace est principalement considéré sous l'angle de son pouvoir transformateur.

6 – Le cyberespace, un espace relatif et performant métaphore de la sécurité (Thierry Balzacq, Myriam Dunn Cavelty).

Le cyber-incident est défini par Thierry Balzacq et Myriam Dunn Cavelty comme une « déponctualisation de réseaux de cybersécurité par des médiateurs se présentant sous la forme de logiciels malveillants, avec des effets dans les espaces régionaux, en réseau et fluides ». Ici c'est la performance du logiciel malveillant qui fonde l'espace de ce dernier (théorie de la performance des espaces).

En résumé, la région est ce qui ressemblerait le plus à un État au sens classique du terme. Elle est définie par des frontières claires et un tout cohérent. Elle possède un intérieur et un extérieur. Par opposition le réseau n'est pas constitué par sa position dans l'espace, celle-ci existe mais n'est pas déterminante de sa nature. Le réseau contredit le phénomène hiérarchique par une forme d'horizontalité. La région et le réseau fonctionnent d'une manière semblable du point de vue de la sécurité, chacun de ses espaces recherche la sécurisation de ses points de vulnérabilité aux fins d'assurer sa continuité (donc la conservation relative de la forme de son espace). La fluidité représente l'échec de cette sécurité.

Le cyberespace apparaît comme l'expression de la sécurité ou de l'insécurité des actants membres d'un réseau.

Pistes de réflexion

Au-delà de ces résultats, la thèse appelle quelques remarques sur ses limites et sur les perspectives qui s'en dégagent.

Du point de vue des limites, la thèse est contrainte par la délimitation de la problématique à combiner une épistémologie complexe avec une approche synthétique qui dégradera sans doute à la complexité de la pensée de certains auteurs de l'ensemble des œuvres étudiées. Du travail théorique résulte également une complexité des notions et des concepts abordés dans cette thèse (le même mot ne signifie pas forcément la même chose en fonction de la partie où il se trouve).

Le fait d'avoir sélectionné des textes en français a limité la possibilité de réaliser des approches quantitatives et comparatives. Bien que cela n'était pas strictement nécessaire pour répondre à la problématique. Une perspective intéressante pourrait être d'opérer un traitement statistique à partir de l'anglais, cependant, les langues anglaises varient à travers le monde et une étude comparative de ce genre pourrait sans doute se voir opposer quelques divergences d'un État anglophone à l'autre. Toutefois, même si le traitement des données appliqué dans cette thèse ne permet pas de recourir à la comparaison. Les mérites de telles approches demeurent sur un objet comme la sécurité de l'information.

Du point de vue des perspectives, il serait intéressant d'approfondir plusieurs points de cette recherche, en particulier les quatre questions du quatrième chapitre qui ouvrent de vrais champs de réflexion sur la discipline des Relations Internationales qui permettrait de tenter d'enrichir l'approche du cyberspace au-delà des seules questions de sécurité ou de travailler sur d'autres objets que l'information. Un autre point qui pourrait être intéressant serait de reprendre l'ensemble des données récoltés au cours du terrain afin de conduire une analyse de la communauté épistémique en passant par une sociologie du milieu français de la recherche en cybersécurité.

Toutefois, le moyen le plus évident de poursuivre une telle recherche semble ici de trouver d'autres théories pour compléter la sélection du dernier chapitre. L'une des approches les plus prometteuses pour améliorer le texte explicatif idéal de l'objet étudié semble être les modèles d'acteurs en réseaux tirés de la sociologie des réseaux complexes.

Table des matières.

Tome 1

Convention d'écriture	4
Réserve de responsabilité	4
Remerciements	5
Sommaire	7
Liste des illustrations	10

Introduction générale.....12

Des récits « officiels » à dépasser : le réveil « cyber » de la « nuit de bronze » (Estonie, avril-mai 2007).....	14
Une mise en récit insérée dans une succession d'évènements entre 2005 et 2008 : de la gouvernance d'Internet à la lutte informatique	16
Problématique de la recherche.	19
Architecture de la thèse.	21

Chapitre liminaire – Stratégie, méthode et conduite de la recherche.24

Section 1 – Théories des Relations Internationales : des paradigmes à la combinaison pragmatique.....26	
A – Un contexte général non-consensuel et polysémique : théories et grands débats « inter-paradigmatiques ».	28
1 – La conversation scientifique et l'organisation des théories des Relations Internationales.	30
2 – Les grands débats, la classification des théories générales et débats sectoriels.....	34
3 – Rejet, monisme et pluralisme : des approches <i>theory-driven</i> aux approches <i>problem-driven</i>	40
B – Approches éclectiques et objets complexes : le pragmatisme « <i>problem-driven</i> ».....	42
1 – Le pragmatisme conduit par les problèmes : à la recherche du texte explicatif idéal.....	45
2 – Réunir des théories contradictoires : L'érotétique ou la logique des questions.	46
3 – L'inclusion et l'exclusion des théories par la sélection pragmatique.....	47

Section 2 – Les mots et les discours : De l’efficacité politique du langage à l’objectivation rhétorique du politique	50
A – Penser le discours comme objet politique pour les Relations Internationales : une mosaïque de théories, d’outils et de postures.....	53
B - Approches discursives de la sécurité : entre réalismes, constructivismes et poststructuralismes.....	58
1 – Le discours et l’élargissement du concept de sécurité : de la théorie critique aux constructivismes	61
2 – Langage, discours et approches poststructuralistes de la sécurité.....	66
3 – Les théories de la « sécurisation » : des « classiques » aux « critiques »	67
C – Epistémologie du discours chez Jean-Claude Passeron : comprendre la prolifération des mots dans et hors « la cité des sciences ».....	74
1 – Nature du langage et conversation scientifique : le rejet épistémique de la forme logique de la réfutation.....	75
2 – Espace sémantique, occurrences et évènements.	78
3 – Concepts polymorphes et sténographiques face à la circulation des idées dans l'espace sémantique.....	80
4 – Epistémologie de Jean-Claude Passeron et Relations Internationales	82
Section 3 – Dépasser le nominalisme : Etude de discours et approche phénoménologique plurale du « cyberespace ».....	83
A – Des récits à l’histoire des idées : éléments pour une généalogie du cyberespace.	84
B – Impact normatif du cyberespace et des termes dérivés : bases de données, observation statistique et analyse logométrique.....	86
1 – Outils conceptuels pour l’emploi d’une approche logométrique.	88
2 – Impact normatif et sélection des corpus.....	90
3 – Optimisation de moteurs de recherche : développement de l’agent logiciel GnOSIE.	93
C – A la recherche de l’objet scientifique « cyber » en France : de la communauté discursive à la communauté épistémique ?	94
1 – La communauté : concept polymorphe.	96
2 – La communauté discursive : situer la communauté dans l’espace sémantique.....	98
3 – La communauté épistémique : production et influence communautaires.	99

Section 4 – Entre phénomène discursif et combinaison pragmatique, l’apport d’une méthode de travail abductive.	104
Section 5 – Du doctorant à l’officier : regard critique sur un parcours doctoral engagé.	108
Section 6 – Evolution des contraintes matérielles et scientifiques de la recherche.	113
A – Contraintes matérielles du projet.....	113
1 – Financement de la thèse.	114
2 – Mobilité géographique.	115
3 – Les contraintes temporelles.	115
B – Difficultés rencontrées dans le travail de recherche	116
1 – Légitimité d’objet et légitimité disciplinaire pour traiter l’objet.	116
2 – Les effets de l’actualité de l’objet « cyber » sur la production des résultats.....	117
3 – L’exploitation des entretiens : sources d’informations et résultats exploitables.....	117
4 – L’accès aux sources bibliographiques et faiblesse des sources archivistiques.	119
Partie I – Du mot au discours, le tournant sécuritaire du cyberespace : Eviter les pièges de la recherche d’une définition unique.	122
Chapitre 1 – Circulations et mutations du cyberespace : un objet hors de la technique ?	124
Section 1 – Aux sources du pouvoir évocateur du cyberespace, invention, héritages et confusions.	128
A – Invention et définition du terme cyberespace entre 1982 et 1984 : la littérature d’anticipation dystopique.	129
1 – Le cyberespace de William Gibson.....	130
2 – Le phénomène « cyberespace » dans le langage.	132
B – Le cyberespace comme revendication d’un héritage scientifique et culturel.	134
1 – L’héritage de la pensée systémique et le mouvement cybernétique.	136
2 – L’héritage des premières appropriations de la cybernétique : le « cyborg » et la « guerre cybernétique ».	138

C – Cyberespace et définition(s) technique(s) : Déconstruire les idées reçues.....	140
1 – Confusion(s) sur le cyberespace : la « Toile » et les « sphères » de l'information.....	141
2 – Cyberespace et objet « Internet » : les origines d'Internet et du « Web ».....	143
3 – Discontinuité entre cyberespace et information : Infosphère et sphère informationnelle.	
.....	144
Section 2 – Le cyberespace comme discours ambigu sur les technologies de l'information.	
.....	146
A – Penser les rapports entre la technique et la société.....	148
1 – Les postures intellectuelles face à la technique : système, causalités et réseau.....	150
2 – La technique comme phénomène social et « international » : nation et civilisation chez Marcel Maus.....	156
B – Information et technologie : un héritage matérialiste à dépasser.	162
1 – De la « structure » à la « fonction » : les origines matérialistes de l'information.....	162
2 – Information et progrès technique : le rôle clef des technologies de l'information.....	164
C – Structure d'une fiction techno-politique : le pouvoir évocateur du cyberespace.	169
1 – Les « utopies » du cyberespace : la spatialisation comme représentation simplifiée et totale de l'information.....	171
2 – La sécurité, la réponse « pragmatique » à la non-maitrise de l'information.	178
3 – Fétiches du discours : objets techniques répétitifs et personnages conceptuels.....	180
Section 3 – Une nécessaire méfiance envers les tentatives de définitions du cyberespace et des termes dérivés.	183
A – Le caractère non-souhaitable d'une définition technique du cyberespace.	186
1 – La définition du cyberespace : une information apparemment peu utile.	187
2 – Idée de menace et précautions nécessaires vis-à-vis des « discours catastrophistes » à partir des années 2000.....	188
B – Le piège de la technique et employabilité des notions dérivées du cyberespace : l'exemple de la cyberarme.	191
Conclusions de chapitre.	194

Chapitre 2 – Cyberespace et termes dérivés : analyse logométrique multiniveaux entre 2001 et 2016.....197

Section 1 – Discours « cyber » et impact normatif des enjeux sécuritaires de l’information (France, UE, ONU).....199
A – Analyse du journal officiel de la République française entre 2001 et 2016.....200
1 – Analyse des résultats du recensement (Corpus 1).....203
2 – Résultats des approches thématiques : mondes lexicaux et analyse de similitude (Corpus 1).....208
B – Analyse du journal officiel de l’Union Européenne en français entre 2001 et 2016....210
1 – Analyse des résultats du recensement (Corpus 2).....213
2 – Résultats des approches thématiques : mondes lexicaux et analyse de similitude (Corpus 2).....217
C – Analyse documents de l’ONU de l’Organisation des Nations Unies en français entre 2001 et 2016.....218
1 – Analyse des résultats du recensement (Corpus 3).....221
2 – Résultats des approches thématiques : mondes lexicaux et analyse de similitude (Corpus 3).....225
D – Synthèse des résultats 2001-2016 sur les corpus 1, 2 et 3 :.....226
1 – Recensement d’occurrences - variations des termes « cyber » :226
2 – Classifications hiérarchiques descendantes :.....229
3 – Analyses de similitudes – principaux substantifs :.....230
Section 2 – La thématique « cyber » dans la presse écrite francophone :.....231
A – Résultats à partir du moteur de recherche Factiva.....232
1 – Analyse des résultats du recensement (Corpus 4).....234
2 – Résultats des approches thématiques : mondes lexicaux et analyse de similitude (Corpus 4).....238
B – Résultats à partir de Google News à l’aide de l’agent logiciel GnOSIE.239
1 – Analyse des résultats du recensement (Corpus 5).....242
2 – Résultats des approches thématiques : mondes lexicaux et analyse de similitude (Corpus 5).....246

Section 3 - Eléments de discussion du phénomène discursif « cyber ».....	247
A – Une vie internationale mésestimée au profit d'une position privilégiée de l'acteur régalien dans le discours	251
1 – L'État comme acteur principal pour lutter contre la menace « transnationale » de la cybercriminalité.....	252
2 – Une spécificité normative « réservée à l'État » : la défense comme domaine régalien.	254
3 – L'absence relative de l'individu des centres d'intérêt de l'État : spécificité régaliennes ou spécificité française ?	258
B – Discrimination des enjeux politiques de l'information : les enjeux portés par le discours « cyber ».....	259
1 – Enjeux principaux : menace, protection, sécurité, criminalité, défense	260
2 – Enjeux périphériques : gouvernance, gestion des flux de données, résilience.....	263
Conclusions de chapitre.....	266
Chapitre 3 – Le phénomène linguistique « cyber » : la communauté épistémique comme communauté discursive.....	268
Section 1 – De l'émergence de la production d'une communauté épistémique dans le champ sémantique.....	269
A – Critère de présence de la communauté épistémique : de l'intégration à la production.	270
1 – De la connaissance scientifique à la connaissance experte.	272
2 – La connaissance face au paradoxe du professionnalisme communautaire	273
B – Critères d'influence d'une communauté épistémique.	275
1 – Le principe d'incertitude comme condition fondamentale de l'influence communautaire.	275
2 – Une influence politique déterminée par des conditions structurelles et processuelles...	277
3 – Une influence alimentée par la cohérence de la communauté.	279
C – Discours et communauté épistémique : influence, controverse et concurrence.	280
1 – Influence communautaire : des influences « logiques » sur le « monde historique »....	282
2 – Des controverses dans la communauté épistémique : concurrence et influence dans l'espace sémantique.....	283

Section 2 - Les frontières normatives de la sécurité de l'information.....	285
A - La diffusion de l'enjeu de sécurité de l'information dans le monde.....	285
1 – Des frontières plus étendues que les limites imposées par la technique.	288
2 – Le poids du contexte national dans la production des communautés épistémiques.....	289
B – La différenciation par le contenu des discours.	291
1 – Les frontières induites par le discours « sécurité de l'information – cyber – État » : critères matériel et formel.	293
2 – Les liens bureaucratiques comme source de division au sein de la communauté.....	298
C – Influences politiques au sein de la couche technique d'Internet.	300
1 – Gouvernance et controverses du contrôle technique d'Internet.	301
2 – Le rôle de l'expert technique dans les relations transnationales en matière de sécurité : l'exemple des CSIRT.	303
 Section 3 – La place du phénomène linguistique « cyber » dans les enjeux de sécurité de l'information en France.	305
A – Les sources du langage « cyber » : une idée anglo-saxonne en France ?.....	306
1 – La cyberguerre ou le mythe de la révolution stratégique : la RAND Corporation.	307
2 – Le modèle des « couches » pour décrire le cyberespace.	309
3 – La controverse autour de l'élaboration des <i>Manuels de Talinn</i>	311
B – L'émergence de la sécurité de l'information avant la mode du Cyberespace en France.	313
1 – Les origines de l'informatique et de la sécurité informatique en France.	313
2 – Les premières publications en français associant sécurité de l'information, cyber et État.	317
C – La transformation de la sécurité de l'information en enjeux de sécurité nationale.....	321
1 – Consécration de la sécurité de l'information par le Livre blanc de 2008.....	321
2 – Le langage « cyber » et la sécurité dans les textes antérieurs à 2008.	322
D – La recherche en France face au tournant sécuritaire du cyberespace.....	325
1 – Limites du terrain : fractures de la recherche « cyber » en France.	325
2 – Les chaires de recherche « cyber » : « L'âge d'or », 2012 – 2017.	328
3 – Les aspects sociaux des évènements scientifiques, source d'influence communautaire.	331

Conclusions de chapitre.....	333
-------------------------------------	------------

Conclusions partielles.....	335
------------------------------------	------------

Tome 2

Partie II – Sécurité de l'information dans les Relations Internationales : De l'enjeu de sécurité à un acteur en réseau.....	343
---	------------

Chapitre 4 – Le cyberspace, un discours de sécurité consacré à l'information parmi d'autres.....	345
---	------------

<i>Section 1 – Des éléments du discours : menace, dépendance, valorisation de l'information.</i>	
.....	346

A – Définition discursive de la menace et désignation de l'adversaire : une synthèse globale de nombreux enjeux de sécurité.....	347
--	-----

1 – Des caractéristiques de la menace, entre importance et incertitude.....	347
---	-----

2 – L'imaginaire victimaire et nécessité d'action : enjeux de légitimation des acteurs.....	353
---	-----

B – Des éléments concret de la menace : la dépendance à l'information.....	356
--	-----

C – Valorisation et capitalisation de l'information : de l'inégalité des acteurs en termes d'information.....	359
---	-----

Section 2 – Théories pour une approche discursive du cyberspace et de la sécurité de l'information.....	364
---	-----

A – L'impact de la sécurisation : la cybersécurité comme secteur autonome ?	365
---	-----

1 – La pluralité des discours sur Internet et objets référents : la typologie de Deibert	366
--	-----

2 – Les « grammaires » de la cybersécurité : l'hypersécurisation, les pratiques quotidiennes de sécurité et les technifications.....	369
--	-----

B – Une illusoire autonomie de la sécurité face aux limites du discours.....	372
--	-----

1 – L'approximation du langage : l'exemple de la critique du cyberterrorisme de Conway.	373
--	-----

2 – Controverses du langage et sécurité de l'information.....	375
---	-----

C – Recontextualisation de la sécurisation de l'information.	377
---	-----

1 – Le « cyber- », un label comme les autres ? Les conflits postmodernes de Gray.	378
2 – La sécurité à l'âge digital chez Der Derian.	383
3 – L'identité et la transformation globale de la sécurité de Dartnell.	386
Section 3 – La réception des discours sur la sécurité de l'information dans les Relations Internationales.....	388
A – Approches générales des technologies de l'information et Théories des Relations Internationales.	390
1 – Le déterminisme technique inhérent au développement des Relations Internationales. 391	
2 – Impact des approches paradigmatisques des technologies de l'information.	394
3 – Récits et conceptualisations du cyberspace dans les Relations Internationales.	397
B – La technologie et la sécurité, entre influence normative et partage du pouvoir.....	401
1 – Gouvernance et Internet : un modèle de participation ?.....	402
2 – La société civile globale et prise en compte des réseaux transnationaux.....	409
3 – Les technologies de l'information et sécurité dans le développement.....	413
4 – L'impact de la technologie sur les régimes politiques : le cas des régimes autoritaires.	416
5 – Le concept de Cyberpower et les Relations Internationales.....	418
6 – Les normes de cybersécurité par rapport à la description de la menace.	420
C – La technologie et la sécurité, source de conflictualité.....	422
1 – La cyberguerre dans la guerre conventionnelle.....	423
2 – Cyberspace, un nouvel équilibre entre l'offensive et la défensive.....	426
3 – Les tentatives de conceptualisation d'une cyberdissuasion.	428
4 – Technologies de l'information et transformation des organisations militaires.	430
Conclusions de chapitre.	432
Chapitre 5 – Au-delà du discours, étudier les Relations Internationales par la sécurité de l'information.	435
Section 1 – Les questions de la sécurité de l'information aux Relations Internationales.....	436
A – La question du langage : l'utilisation du langage « cyber ».	438

1 – Les « faiblesses » du langage « cyber ».....	438
2 – L’alternative au langage du cyberspace.....	441
B – La question de la technologie : les apports de la sociologie des sciences et techniques.	
.....	443
1 – Théorie critique des technologies : penser le développement inégal et la domination. .	444
2 – Construction sociale des technologies de l’information et Relations Internationales....	447
3 – Nouveaux matérialismes : réalisme spéculatif, post-humanisme et philosophie orientée objet.....	451
4 – Théorie de l’acteur-réseau et technologie dans les Relations Internationales.....	453
C – La question de l’agentivité : pluralité et diversité des acteurs.....	456
1 – Les contours de l’agentivité en Relations Internationales.....	457
2 – Agentivité, asymétrie et sécurité de l’information.	458
D – L’information en tant qu’objet : vers les Relations Internationales « computationnelles ».	
.....	460
Section 2 – Comprendre la sécurité de l’information dans l’étude des Relations Internationales.....	463
A – Les théories « cyberpolitiques » des Relations Internationales.....	464
1 – Les cyberpolitiques et le « <i>Cyber - IR System</i> » : le domaine politique du cyberspace.	
.....	465
2 – Les théories de la pression latérale et du réalignement latéral.	468
3 – Le dilemme de la coévolution et les phénomènes complexes.....	471
B – Vers une casuistique de la cybersécurité : l’apport de la théorie de l’acteur-réseau.	473
1 – Le concept de « cyber-incident ». ..	474
2 – Application de la théorie de l’acteur-réseau : topologie et sécurité.	475
3 – Le langage « cyber » comme réponse à l’ignorance.	477
Conclusions de chapitre.	478
Conclusion générale.	481
Retour sur la démarche de recherche.	481
Entre discours et sécurité de l’information, comprendre le cyberspace dans les Relations Internationales.	484

Pistes de réflexion	489
Table des matières	490
Sources.....	501
Bibliographie.....	513
Index des noms d'auteurs	560

Sources.

Traitement statistique et bases de données.

1. Corpus 1 « *Cyber JO RF 2001-2016* ».

L'ensemble des publications du journal officiel de la République française entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé. (52 textes retenus).

Base de données :

LEGI: Codes, lois et règlements consolidés, créée en 2014, mise à jour : aout 2017.
Données extraites en septembre 2017 (version texte).

Licence ouverte.

2. Corpus 2 « *Cyber JO UE 2001-2016* ».

L'ensemble des publications du journal officiel de l'Union Européenne entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé. (164 textes retenus).

Base de données :

EUR-LEX : Législation de l'UE, créée en 1997, ouverte au public en 2001, mise à jour d'aout 2017. Données extraites en septembre 2017.

© Union européenne, <http://eur-lex.europa.eu/>, 1998-2017.

3. Corpus 3 « *Cyber DOC ONU 2001-2016* ».

L'ensemble des publications du système de diffusion électronique des documents de l'ONU en français entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé. (218 textes).

Base de données :

Système de diffusion électronique des documents (Sédoc) de l'Organisation des Nations Unies, créé en 1993, mise à jour : aout 2017. Données extraites en septembre 2017.

Tous droits réservés « © Organisation des Nations Unies, <https://www.un.org/>, 1993-2017 ».

4. Corpus 4 « *Cyber Fact FR 2001-2016* ».

L'ensemble des publications francophones de presse généraliste et spécialisée entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé disponibles sur la plateforme Factiva. (27957 textes retenus)

Base de données :

Factiva, créée en 1999, mise à jour décembre 2017. Données extraites en décembre 2017.

Tous droits réservés « © Dow Jones 2017 ». Les éléments de presse recensées sont la propriété exclusive d'éditeurs tiers.

5. Corpus 5 « *Cyber Google News GnOSIE FR 2001-2016* ».

L'ensemble des publications francophones de presse généraliste et spécialisée entre 2001 et 2016 contenant le mot cyberspace ou un terme dérivé sur la base de données de Google News. (20362 textes retenus)

Base de données :

Google News, créé en septembre 2002, mise à jour décembre 2017. Données extraites en décembre 2017.

Tous droits réservés « © Google 2017 ». Les éléments de presse recensées sont la propriété exclusive d'éditeurs tiers.

Liste des colloques, conférences, réunions et autres évènements à caractère scientifique observés.

(*) *Evénements avec une participation dans l'organisation ou/et une présentation.*

Cette liste représente l'ensemble des évènements à caractère scientifique lié au cyberespace ou à la sécurité de l'information observés durant la période de thèse entre 2012 et 2018. Les évènements sans rapport direct avec le cyberespace ne sont mentionnés qu'à raison d'une présentation personnelle sur l'objet en question. Les autres évènements scientifiques intervenus au cours de la thèse en sont exclus.

Année 2012

1. 23 novembre 2012. « Réflexions plurielles sur le cyberconflit » journée qui s'inscrit dans le cadre du programme du GERN - Groupe Européen de Recherches sur les Normativités - Laboratoire CESDIP - CNRS/UVSQ/Min. de la Justice).

Année 2013

2. 7 février 2013. Première séance de travail du groupe de réflexion sur les données personnelles du réseau Trans-Europ Experts (RFID/Cookies/définition du caractère personnel d'une donnée). Cadre d'élaboration d'un rapport concernant un projet d'une future directive européenne sur ces données et leur commerce dans l'Union (Com2012 /11). IRJS, Paris.
3. 26 mars 2013. Séminaire Jeunes Chercheurs sur le « Cyber ». Chaire Castex de Cyberstratégie. IHEDN, école militaire.
4. 15 avril 2013. "Journée de l'Europe" Lutte contre la contrefaçon. Cedre. Université de Rennes 1.
5. 28 avril 2013. "Comment se délimitent et s'imbriquent les différents niveaux de réalité : virtuelle, augmentée, fictionnelle ?" Rennes, Beaulieu, INSA, Halle Francis Querné.
6. 28 mai 2013. Séminaire Jeunes Chercheurs sur le Cyber Chaire Castex de Cyberstratégie. IHEDN, école militaire. Paris.
7. 28 mai 2013. Conférence de Nicolas Ruff, Chercheur en sécurité informatique au sein de la société EADS (Cassidian Cybersécurité). Chaire Castex de Cyberstratégie. IHEDN, école militaire.

8. 4 juin 2013. « Les frontières du cyberspace ». Une journée d'études organisée par le Centre de recherche des écoles de Saint-Cyr Coëtquidan organise, avec le soutien de la Chaire de Cyberdéfense et Cybersécurité Saint-Cyr Sogeti Thales, Musée de l'école des transmissions, Cesson-Sévigné.
9. 25 juin 2013. « Nouvelles technologies et crime désorganisé : Incursion au cœur d'un réseau de pirates informatiques » Conférencier : Benoit Dupont, Professeur, Directeur du CICC (Université de Montréal) Chaire de Cyberdéfense et Cybersécurité Saint-Cyr Sogeti Thales, école militaire, Paris.
10. 26 juin 2013. Séance dédiée aux Big Data du groupe de réflexion sur les données personnelles du réseau Trans-Europ Experts. Cadre d'élaboration d'un rapport concernant un projet d'une future directive européenne sur ces données et leur commerce dans l'Union (Com2012 /11). IRJS, Paris.
11. 1er juillet 2013. « Comprendre les stratégies et politiques de Cybersécurité et de Cyberdéfense de la Chine » Journée-conférence organisée par la Chaire de Cyberdéfense et Cybersécurité Saint-Cyr Sogeti Thales à l'Hôtel National des Invalides.
12. 18 septembre 2013, 1^{er} Symposium Académique National de recherche en Cyberdéfense. DAS, IRSEM, Réserve Citoyenne Cyberdéfense, à l'Ecole militaire. Paris.
13. 8 octobre 2013. Journée d'étude Le droit et l'éthique face aux défis de la Cyberconflictualité ». 8 octobre 2013. Chaire de Cyberdéfense et Cybersécurité Saint-Cyr Sogeti Thales, école militaire, Paris.
14. 15 octobre 2013. Séminaire Jeunes Chercheurs sur le « Cyber ». Chaire Castex de Cyberstratégie. IHEDN, école militaire. Paris.
15. 12 novembre 2013. Séminaire Jeunes Chercheurs sur le « Cyber ». Chaire Castex de Cyberstratégie. IHEDN, école militaire. Paris.
16. 12 décembre 2013. Séminaire Jeunes Chercheurs sur le « Cyber ». Chaire Castex de Cyberstratégie. IHEDN, école militaire. Paris.

Année 2014

17. 12 mars 2014. Journée d'étude « Cyberconflictualité et forces armées ». Chaire de Cyberdéfense et Cybersécurité Saint-Cyr Sogeti Thales, Rennes.

18. (*) 13 et 14 mars 2014. Colloque « Le monde après Snowden » organisé par le Séminaire Jeunes Chercheurs, Chaire Castex de Cyberstratégie, IFG, Paris 8, Salle Victor Hugo, 101, rue de l'université, Paris.
19. 12 septembre 2014. « Droits et souverainetés à l'âge de l'Internet : quels défis pour l'Europe ? », organisé dans le cadre de la Chaire européenne Jean Monnet « Union européenne et société de l'Information » de Télécom Bretagne avec le concours de la chaire de Cyberdéfense et Cybersécurité Saint-Cyr / Sogeti / Thales, à l'Hôtel de Rennes Métropole.
20. (*) 25 et 26 septembre 2014. colloque Fiction et sciences sociales - Bonnes et mauvaises fréquentations, organisé par le CESSP (Paris 1 / EHESS) au Conservatoire National des Arts et Métiers, Paris.
Intervention. « L'interdépendance des sciences sociales et de la fiction dans l'évolution des objets sociaux : L'exemple du cyberespace »

Année 2015

21. (*) 8 septembre 2015. Journée d'échanges au sein de la communauté Cyb'Air.
Intervention : « Une ébauche de définition du cyberespace ».
22. (*) 16 et 17 septembre 2015. Colloque "La performance", IDPSP, Rennes.
Intervention : « Cyberespace et performance: normes, externalisation, contraintes ».

Année 2016

23. 5 avril 2016. Séminaire « Cyber vulnérabilité des systèmes d'information liés à la logistique et à la maintenance de la Défense » Musée des Transmissions à Cesson-Sévigné, par la chaire de Cyberdéfense et Cybersécurité Saint-Cyr.
24. 7 avril 2016. « 2e rencontres parlementaires cybersécurité & milieu maritime », à la Fédération française du bâtiment, Paris, 17ème.
25. 25 mai 2016. Journée cybercriminalité, FMSH, Paris, programme « Usages des nouvelles technologies dans les domaines de la sécurité et de la justice pénale » par le GERN.
26. 7 juillet 2016 « Geopolitics of Cyber in Asia », organisé par la Chaire Castex en partenariat avec l'EastWest Institute, l'Institut Français de Géopolitique (Paris 8 -

Vincennes / Saint-Denis) et Asia Centre, ainsi qu'avec le parrainage du FIC 2017.
Société de Géographie, 184 Boulevard Saint-Germain, Paris.

Année 2017

27. (*) 24 mars 2017. Réunion du comité scientifique de la Chaire « Cyber résilience aérospatiale ».
Intervention : Présentation de thèse
28. (*) 22 novembre 2017. Conférence « Le cyber-espace, nouveau théâtre de guerre ? »,
Association ELSA, faculté de droit d'Aix.
Intervention : « Le cyberspace dans les Relations Internationales »,
29. (*) 13 et 14 décembre 2017. Colloque annuel de l'Association pour les Études sur la Guerre et la Stratégie.
Intervention : « Cyberespace et enjeux politiques de l'information : quelle place pour le soldat ? (2001 –2016) ».

Année 2018.

30. 11 janvier 2018. Leçon inaugurale Chaire « Cyber résilience aérospatiale » (Thales et Dassault Aviation). Centre de recherche de l'Armée de l'air. Base aérienne 701 de Salon-de-Provence.
31. (*) 21 au 26 juillet 2018. IPSA World Congress of Political Science, Brisbane, Australie.
Intervention : « Ending Cyberspace's Myth of Universality : Information's Security Stakes beyond Borders (2001-2016) ».
32. (*) 29 Novembre 2018. Journée de recherche « Cyber Résilience des systèmes et des organisations », Ecole Militaire, Paris.
Intervention : « Cyber-Résilience, une analyse discursive ».

Liste anonymisée d'entretiens réalisés en cours de thèse.

23 novembre 2012.

Fonction de la personne interrogée : officier supérieur français délégation aux affaires stratégiques du Ministère de la Défense.

Lieu : Gare de Lyon, Tour de l'Horloge 4, place Louis Armand, Paris.

Durée : 21 minutes.

Type d'entretien : non-directif.

23 novembre 2012.

Fonction de la personne interrogée : enseignant-chercheur français, Université Paris IV

Lieu : Gare Montparnasse, Paris.

Durée : 48 minutes.

Type d'entretien : non-directif.

7 février 2013.

Fonction de la personne interrogée : ingénieur général des Mines, membre du Collège de la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi).

Lieu : Locaux de l'IEJ de l'université Paris 1 Panthéon-Sorbonne

Durée : 28 minutes.

Type d'entretien : non-directif.

25 juin 2013.

Fonction de la personne interrogée : officier supérieur français détaché dans un think tank français.

Lieu : Ecole militaire, Paris.

Durée : 29 minutes.

Type d'entretien : non-directif.

18 septembre 2013.

Fonction de la personne interrogée : officier supérieur délégation aux affaires stratégiques du Ministère de la Défense.

Lieu : Ecole militaire, Paris

Durée : 32 minutes.

Type d'entretien : non-directif.

18 septembre 2013.

Fonction de la personne interrogée : officier supérieur français adjoint à l'officier lutte informatique défensive.

Lieu : Ecole militaire, Paris

Durée : 23 minutes.

Type d'entretien : non-directif.

13 mars 2014.

Fonction de la personne interrogée : conférencier, hacker (Chaos Computer Club, Suisse)

Lieu : Salle Victor Hugo, 101, rue de l'université, Paris.

Durée : 45 minutes.

Type d'entretien : non-directif.

9 juillet 2014.

Fonction de la personne interrogée : secrétaire des affaires étrangères chargé de la cybersécurité à la direction générale des affaires politiques et de sécurité du Ministères des affaires étrangères français.

Lieu : Ministère des affaires étrangères, Paris.

Durée : 1 heure 28.

Type d'entretien : non-directif.

11 juillet 2014.

Fonction de la personne interrogée : ingénieur de recherche au CNRS, titulaire de chaire.

Lieu : Café Ciel de Paris, Tour Montparnasse, Paris.

Durée : 2h05.

Type d'entretien : non-directif.

12 septembre 2014.

Fonction de la personne interrogée : enseignant-chercheur français, Université de Toulouse 1 et 2.

Lieu : Hôtel de Rennes Métropole.

Durée : 35 minutes.

Type d'entretien : déjeuner, non-directif.

9 juin 2015.

Fonction de la personne interrogée : directeur adjoint des affaires stratégiques, de sécurité et du désarmement de la direction générale des affaires politiques et de sécurité du Ministères des affaires étrangères français.

Lieu : Café Le Pierrot, Avenue de la Motte-Picquet, Paris

Durée : 1 heure 37.

Type d'entretien : déjeuner, non-directif.

16 juillet 2015.

Fonction de la personne interrogée : directeur de la National Security Agency et de l'US Cyber command.

Lieu : Ecole militaire, Paris.

Durée : 1h05

Type d'entretien : directif et collectif (séminaire jeunes chercheurs de la chaire Castex).

16 juillet 2015.

Fonction de la personne interrogée : officier supérieur français IRSEM.

Lieu : Ecole militaire, Paris.

Durée : 30 minutes.

Type d'entretien : non-directif

5 avril 2016.

Fonction de la personne interrogée : officier supérieur français, chef de bureau au SHAPE, OTAN.

Lieu : Ecole des transmission, Cesson-Sévigné, Rennes.

Durée : 30 minutes.

Type d'entretien : non-directif.

25 mai 2016.

Fonction de la personne interrogée : consultant, expert judiciaire en cybercriminalité.

Lieu : Café sur l'herbe, Gare de Lyon, Paris

Durée : 1 heure 30.

Type d'entretien : non-directif.

Rapports officiels cités.

- CONSEIL D'ÉTAT, Internet et les réseaux numériques, Paris, La documentation française, 1998, 193 p.
- WORLD ECONOMIC FORUM , The Global Risks Report, 13ème édition, 2018.
- BOCKEL Jean-Marie, La cyberdéfense : un enjeu mondial, une priorité nationale, Sénat, 18 juillet 2012.
- BRETON Thierry, Les Téléservices en France. Quels marchés pour les autoroutes de l'information ?, rapport au ministre de l'Intérieur et de l'Aménagement du territoire, et au ministre des Entreprises et du Développement économique, Paris, La Documentation française, 1994, 615 p.
- GAUTRAUD Nathalie et FALQUE-PIERROTIN Isabelle, Internet: Enjeux Juridiques. Rapport au ministre délégué à la Poste aux Télécommunications et à l'Espace et au ministre de la Culture, Paris, La Documentation Française, 1997.
- LABORDES Pierre La Sécurité des systèmes d'information - Un enjeu majeur pour la France, Paris, La Documentation française, Collection des rapports officiels, janvier 2006, 195 p.
- MARTIN-LALANDE Patrice, L'Internet : un vrai défi pour la France, rapport au Premier Ministre, Paris, La Documentation française, 1997, 89 p.
- MILEO Thierry (dir.), Les réseaux de la société de l'information, Rapport du commissariat général du plan, Groupe de travail Réseaux de la société de l'information, Paris, La Documentation française, 1996, 230 p.

- ROMANI Roger, Cyberdéfense,: un nouvel enjeu de sécurité nationale, Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées, n° 449, juin 2008
- THERY Gérard, Les autoroute de l'information, rapport au Premier Ministre, Paris, La Documentation française, Janvier 1994, 98 p.

Doctrine juridique citée.

- SCHMITT Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017, 638 p.
- SCHMITT Michael N., *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013, 304 p.

Discours officiels cités.

- PANETTA Leon E., « Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City », 11 octobre 2012.
- Déclaration de principes WSIS-03/GENEVA/DOC/4-F, *Construire la société de l'information : un défi mondial pour le nouveau millénaire*, sommet mondial sur la société de l'information, Genève, 12 mai 2004, article 35.
- Communiqué G7/P8 « Meeting of Justice and Interior Ministers of The Eight December 9-10 », Washington, 10 décembre 1997.

Normes et textes officiels spécifiquement cités.

Cette section ne reprend pas l'intégralité des normes et textes officiels utilisés dans cette thèse, mais uniquement les textes auxquels il est fait référence dans le corps du texte.

France

- MINISTÈRE DE LA DEFENSE, Pacte Défense Cyber, 7 février 2014.
- ANSSI, Défense et sécurité des systèmes d'information, Stratégie de la France, 2012, p. 21.

- CICDE, Concept interarmées de Cyberdéfense de la France. CIA 6-3, juillet 2011, reprise dans les documents législatifs postérieurs analysés.
- CICDE, Concept d'emploi des forces, CIA 01, janvier 2010.
- Instruction interministérielle n°2100/SGDN/SSD du 1er décembre 1975.
- L'instruction générale interministérielle n° 100/DN/ANS du 16 janvier 1962.

- *Décret* n°2009-834 du 7 juillet 2009.
- *Décret-loi* du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions. Il fut modifié par le Décret n°73-364 du 12 mars 1973 puis par Décret n°86-250 du 18 février 1986.

- *Loi* n° 2015-917 du 28 juillet 2015 actualisant la programmation militaire pour les années 2015 à 2019 et portant diverses dispositions concernant la défense.
- *Loi* n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
- *Loi* n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Article 1er.Loi

- *Défense et sécurité nationale : Le Livre Blanc*, Paris, La Documentation française, 2008.
- *Défense et sécurité nationale : Le Livre Blanc*, Paris, La Documentation française, 2013.

- *Question écrite* n° 03127 publiée dans le JO Sénat du 02/10/1997. Réponse publiée dans le JO Sénat du 26/02/1998.
- *Compte rendu* de la réunion de la commission des affaires étrangères, de la défense et des forces armées dans le cadre du projet de loi de finance 2008 du 7 novembre 2007.

États-Unis

- Cyberspace opérations concept capability plan 2016-2018, TRADOC Pamphlet 525-7-8, Fort Monroe, États-Unis, 22 février 2010. (Sur ce point voir en particulier le chapitre 2 du document pp. 8 – 14).

Union européenne

- Décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique.
- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogée le 25 mai 2018.

OTAN

- Glossaire OTAN, AAP-06, Edition 2018, p.192.

Bibliographie.

Traités, manuels et dictionnaires

- BAILLAT Alice, EMPRIN Fabien, RAMEL Frédéric, « Chapitre 12 - Des mots et des discours. Du quantitatif au qualitatif », In. DEVIN Guillaume (dir.) *Méthodes de recherche en relations internationales*. Paris, Presses de Sciences Po, « Relations internationales », 2016, p. 227-246.
- BALZACQ Thierry, CHARILLON Frédéric et RAMEL Frédéric, Manuel de diplomatie, Paris, Science Po, 2018, pp. 245 – 352.
- BALZACQ Thierry et RAMEL Frédéric (dir.), *Traité de Relations Internationales*, Paris, Presses de Science Po, 2013. 1232 p.
- BALZACQ Thierry, *Théories de la sécurité, les approches critiques*, Paris, Presses de Science Po, 2016, 512 p.
- BATTISTELLA Dario (2003), *Théories des Relations Internationales*, 4ème éd., Paris, Presses de Science Po, 2012, 760 p.
- BURCHILL Scott, DEVETAK Richard, LINKLATER Andrew, PATERSON Matthew, REUS-SMIT Christian, TRUE Jacqui, *Theories of International Relations*, New York, Palgrave, 2ème édition, 2001, 322 p.
- BURCHILL Scott, LINKLATER Andrew, DEVETAK Richard, DONNELLY Jack, NARDIN Terry, PATERSON Matthew, REUS-SMIT Christian, TRUE Jacqui, *Theories of International Relations*, New York, Palgrave, 5ème édition, 2013, 396 p.
- CHARAUDEAU Patrick et MAINGUENEAU Dominique, Dictionnaire d'analyse du discours, Paris, Le Seuil, 2002, 661 p.
- GRUA François et CAYROL Nicolas, *Méthode des études de droit*, Paris, Dalloz, 2ème édition, 2011, 132 p.
- COMAN Ramona, CRESPY Amandine, LOUAULT Frédéric, MORIN Jean-Frédéric, PILET Jean-Benoit, HAUTE (VAN) Emilie, *Méthodes de la Science Politique*, Paris, De Boeck, 2016, 224 p.
- MACLEOD Alex « Emergence d'un paradigme hégémonique » In. MACLEOD Alex et O'MEARA Dan (dir.), *Théories des relations internationales. Contestations et résistances*, Montréal, Athéna éditions, 2007, pp. 19-34.

- SABATIER Paul A. « Advocacy coalition framework (ACF) », In. BOUSSAGUET Laurie (éd.), *Dictionnaire des politiques publiques. 3e édition actualisée et augmentée*. Presses de Sciences Po, 2010, pp. 49-57.
- VALERIANO Brandon, et MANESS Ryan C. « International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain » In. BROWN Chris et ECKERSLEY Robyn (éds.), *The Oxford Handbook of International Political Theory*, Oxford University Press, mars 2018, 16 p.

Ouvrages collectifs et chapitres d'ouvrages

- AKRICH Madeleine, « 5. Comment sortir de la dichotomie technique/société. Présentation des diverses sociologies de la technique », In LATOUR Bruno et LEMONNIER Pierre (dir.), *De la préhistoire aux missiles balistiques. L'intelligence sociale des techniques*. La Découverte, 1994, pp. 103-131.
- BALZACQ Thierry, « A Theory of Securitization : Origins, Core Assumptions, and Variants », In. Balzacq Thierry (éd.), *Securitization Theory : How Security Problems Emerge and Dissolve*, New York Routledge, 2001, p. 3.
- BENEDIKT Michael, « Cyberspace: Some Proposals. » In. BENEDIKT Michael (ed.), *Cyberspace: First Steps*. Cambridge, The MIT Press, 1994, p. 119 – 224.
- BELL Daniel, « The Social Framework of the Information Society » in Dertouzos, M.L., Moses Joel . (éds), *The Computer Age : a Twenty-Year View*, Cambridge, MIT Press, 1979, pp 163-211.
- BIGO Didier « L'Europe de la sécurité intérieure : penser autrement la sécurité ». In Le GLOANNEC Anne-Marie (éd.), *Entre Union et Nations : l'État en Europe*. Paris, Presses de Sciences Po. 1998. p. 55 - 90.
- BIGO Didier « When Two Become One: Internal and External Securitisations in Europe ». In KELSTRUP Morten et WILLIAMS Michael Charles (éds), *International Relations Theory and The Politics of European Integration. Power, Security and Community*. Routledge. 2000, pp. 171 - 204.
- BOSSY Thibault, et EVRARD Aurélien. « Communauté épistémique », In. BOUSSAGUET Laurie, JACQUOT Sophie et RAVINET Pauline (dir.), *Dictionnaire des politiques publiques. 4e édition précédée d'un nouvel avant-propos*. Presses de Sciences Po, 2014, pp. 140-147.

- CHAZAL Gérard, « Chapitre 15. La notion d'information et le matérialisme », In. SILBERSTEIN Marc (dir.), *Matériaux philosophiques et scientifiques pour un matérialisme contemporain*, Paris, Editions Matériologiques, vol. 1, 2013, pp. 455-479.
- CALLON Michel et LATOUR Bruno, « Unscrewing the Big Leviathan: how actors macrostructure reality and how sociologists help them to do so », in KNORR-CETINA Karin D. et CICOUREL Aaron V. (éds.), *Advances in Social Theory and Methodology: Toward an Integration of Micro- and Macro-Sociologies*, Boston, Mass, Routledge and Kegan Paul, pp. 277-303.
- CLYNES Manfred et KLINE Nathan S. « Drugs, Space, and Cybernetics: Evolution to Cyborgs » In FLAHERTY Bernard, E. (éd.) *Psychopharmacological Aspects of Space Flight*, New York: Columbia University Press, 1961 pp 345–371 ;
- DAVID Paul, « La moissonneuse et le robot. La diffusion des innovations fondées sur la micro-électronique » In. SALOMON Jean.-Jacques. et SCHMEDER Geneviève (eds) *Les enjeux du changement technologique*, Paris, CPE-Economica, 1986,
- DEIBERT Ronald J. « Circuits of Power: Security in the Internet Environment » In. ROSENAU James N., et SINGH J. P. (eds). *Information Technologies and Global Politics: the Changing Scope of Power and Governance*. State University of New York, 2002, pp. 115 - 142.
- DEMCHAK Chris C, « Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World, » In. BURNS Nicholas et PRICE Jonathan (eds), *Securing Cyberspace: A New Domain for National Security*, Washington, D.C., Aspen Institute, 2012, pp. 59 - 94.
- DESCHAUX-DUTARD Delphine et LAVOREL Sabine (dir.), *Puissances émergentes et sécurité internationale : une nouvelle donne ? Une perspective pluridisciplinaire sur la puissance et l'émergence sur la scène internationale*, Bruxelles, Peter Lang, 2017, 312 p.
- EDKIN Jenny, « Poststructuralism », In. GRIFFITHS Martin (ed.), *International Relations Theory for the Twenty-First Century*, New York, Routledge, 2007, pp. 88-98.
- FEARON James D. et WENDT Alexander, « Rationalism vs constructivism. A Skeptical view » In. CARLSNAES Walter, RISSE Thomas et SIMMONS Beth, *Handbook of international relations*, Sage, 2002, pp 52 – 72.

- HAAS Peter M., « Policy knowledge: epistemic communities ». In SMELSER Neil J. et BALTES Paul B. (eds.), *International Encyclopedia of the Social and Behavioral Sciences*, Elsevier, 2001. p. 11517 - 11578.
- HELD David, « Central Perspectives on the Modern State », In. HELD David et al. (eds.), *States and Societies*, Oxford, Martin Robertson, 1983, pp. 1 -55.
- HELD David, et al. *Global Transformations: Politics, Economics and Culture*. Cambridge, Polity Press, 2001, 602 p.
- HOTTOIS Gilbert. « Chapitre 22. Philosophie de la technique et des technosciences », In. HOTTOIS Gilbert (dir), *De la Renaissance à la Postmodernité. Une histoire de la philosophie moderne et contemporaine*, De Boeck Supérieur, 2005, pp. 485-532.
- KALDOR Mary « The Imaginary War » In. SMITH Dan, et THOMPSON Edward Palmer (dir.). *Prospectus for a Habitable Planet*. Penguin, 1987.
- KATZENSTEIN Peter J. , KEOHANE Robert O. et KRASNER Stephen D. , « International Organization and the Study of World Politics », In. KATZENSTEIN Peter J. , KEOHANE Robert O. et Krasner Stephen D. (dir.), *Exploration and Contestation in the Study of World Politics*, Massachusetts, MIT Press, 1999, pp. 12 - 30.
- KOWERT Paul et LEGRO Jeffrey, « Norms, identity, and their limits : a theoretical reprise » In. KATZENSTEIN Peter (ed.) *The Culture of National Security : Norms and Identity in World Politics*, New York, Columbia University Press pp. 451–497.
- KRAUSE Keith et WILLIAMS Michael C. « From Strategy to Security: Foundations of Critical Security Studies », In KRAUSE Keith et WILLIAMS Michael C. (eds) *Critical Security Studies*, Minneapolis: University of Minnesota Press, 1997, pp. 33-59.
- KREBS Ronald R, « The Limits of Alliance: Conflict, Cooperation, and Collective Identity: Essays on International Relations in Honor of Rich ». In. LAKE Anthony & OCHMANEK David (eds), *The Real and the Ideal: Essays on International Relations in Honor of Rich*, Rowman and Littlefield/Council on Foreign Relation, Lanham, Maryland, 2001 p. 225.
- KUEHL Daniel T., « From Cyberspace to Cyberpower: Defining the Problem » In. KRAMER Franklin D., et al. (dir) *Cyberpower and National Security*. Center for Technology and National Security Policy, 2009, pp. 24–42.
- KURKI Milja et WIGHT Colin, « International Relations and Social Science (Third Edition) ». In. DUNNE Timothy, KURKI Milja et SMITH Steve (dir.), *International*

Relations Theory: Discipline and Diversity, Oxford University Press, 3ème édition, 2013, pp 14-35.

- LA BRANCHE Stéphane. « L'apport de Foucault aux théories des relations internationales : une critique du postmodernisme anglo-saxon ». In. MEYET Sylvain, NAVES Marie-Cécile, et RIBEMONT Thomas; *Travailler avec Foucault. Retours sur le politique*, L'Harmattan, Cahiers Politiques, 2005, pp. 119-139.
- LAMARRE Christiane, « Victime, victimes, essai sur les usages d'un mot », in GARNOT Benoît (dir.), *Les victimes, des oubliées de l'histoire ?*, Presses universitaires de Rennes, 2000, pp 31- 40.
- McCARTHY, Daniel R. (dir), *Technology and World Politics an Introduction*. Routledge, Taylor & Francis Group, 2018., 272 p.
- MASTERTMAN Margaret, « The Nature of a Paradigm », In. Lakatos Imre et Musgrave Alan (dir.), *Criticism and the Growth of Knowledge*, New York, Cambridge University Press, 1970 pp. 61 - 65.
- MAUSS Marcel, « Les civilisations. Eléments et formes » in. Fondation pour la Science - centre international de synthèse (dir.), *Civilisation. Le mot et l'idée*, Paris, La Renaissance du Livre, 1930, pp. 81-108.
- MORAVCSICK Andrew « Liberal International Relations Theory : A Scientific Assessment » In. ELMAN Colin et FENDIUS ELMAN Miriam (eds) *Progress in International Relations Theory: Appraising the Field*, Cambridge, MIT Press, 2003, pp. 159-204
- MUTIMER David, « Critical Security Studies: A Schismatic History » In COLLINS Alan, *Contemporary Security Studies*. Oxford: Oxford University Press, 3ème édition, décembre 2010, pp 53 – 74.
- PAJON Christophe, « Le sociologue enrégimenté : méthodes des sciences sociales en terrain militaire », In. GRESLE François (dir.), *Sociologie du milieu militaire : les conséquences de la professionnalisation des armées et de l'identité militaire*, Paris, L'Harmattan, 2005, pp. 45 – 55
- PERSSON Johannes et PETRI Ylikoski (dir.), *Rethinking Explanation*. Dordrecht, Springer, 2007, pp. 13-26.
- RICHARDSON Jeremy, « Actor Based Models of National and EU Policy-Making: Policy Networks, Epistemic Communities and Advocacy Coalitions » In HUSSEIN Kassim et

ANAND Menon (eds), *The EU and National Industrial Policy*, London: Routledge, 1996, pp. 26–51.

- SABATIER Paul et WEIBLE Christopher M., « The advocacy coalition framework: Innovation and Clarifications » In. SABATIER Paul, *Theories of the Policy Process*, Oxford, Westview Press, 1999 pp 189 – 222.
- SACO Diana. « Colonizing Cyberspace: National Security and the Internet », In. WELDES Jutta, LAFFEY Mark, GUSTERSON Hugh et DUVALL Raymond (eds). *Cultures of Insecurity: States, Communities, and the Production of Danger*, Minneapolis: University of Minnesota Press, 1999, pp. 261-292.
- SCHLANGER Nathan. « 8. Piaget et Leroi-Gourhan. Deux conceptions biologiques des connaissances et des techniques », In LATOUR Bruno et LEMONNIER Pierre (éd.), *De la préhistoire aux missiles balistiques. L'intelligence sociale des techniques*. Paris, La Découverte, 1994, pp. 165-184.
- STARR, Stuart H., « Toward a Preliminary Theory of Cyberpower. » In. KRAMER Franklin D., et al. (dir) *Cyberpower and National Security*. Center for Technology and National Security Policy, 2009, pp. 43–88.
- WÆVER Ole « Securitization and Desecuritization », In. LIPSCHUTZ Ronnie D. (ed.), *Security*, New York, Columbia University Press, 1995,
- WÆVER Ole., « The rise and fall of the inter-paradigm debate », in Smith Steve, Booth Ken., Zalewski Marysia (éds.), *International Theory: Positivism and Beyond*, Cambridge, Cambridge University Press, 1996, pp. 149-185.
- WALKER John, « Through the Looking Glass. Beyond “User Interfaces” », In. LAUREL Brenda (éd.), *The Art of Human-Computer Interface Design*, Boston, Addison-Wesley, janvier 1990, pp. 439 - 448.
- WEEDEN Lisa, « Concepts and commitments in the study of democracy », In. SHAPIRO Ian, SMITH Rogers M., and MASOUD Tarek E. (dir.), *Problems and Methods in the Study of Politics*, Cambridge University Press, 2004. pp. 274 – 306.
- WENDT Alexander, « Anarchy Is What States Make of It. The Social Construction of Power Politics » (1992), in DER DERIAN James (dir.), *International Theory. Critical Investigations*, Basingstoke, Palgrave Macmillan, 1995, pp. 129 -177.
- WOLFERS, Arnold, « National Security as an Ambiguous Symbol » In. WOLFERS, Arnold (Ed.): *Discord and collaboration. Essays on International Politics*, Baltimore: John Hopkins, University Press): pp 147 – 165

- ZEHFUSS Maja, « Constructivisms in International Relations: Wendt, Onuf, and Kratochwil' » In. FIERKE Karin M. et JØRGENSEN Knud Eric (eds), *Constructing International Relations: The Next Generation*, Londres, ME Sharpe, 2001, pp. 54 -75.

Ouvrages et monographies

- COLLECTIF. *Les drones aériens : passé, présent et avenir : approche globale*, CReA, CESA, Paris, La Documentation Française, 2013, 706 p.
- ABELLA Alex, *Soldiers of Reason: The RAND Corporation and the Rise of the American Empire*, Mariner Books, mai 2009, 408 p.
- ACUTO Michele et CURTIS Simon (eds), *Reassembling International Theory. Assemblage Thinking and International Relations*, Londres, Palgrave, 2013, 158 p.
- AKRICH Madeleine, CALLON Michel et Latour Bruno (éd.), *Sociologie de la traduction : textes fondateurs*, Paris, Mines ParisTech, les Presses, « Sciences sociales », 2006, 401 p.
- ALLISON Graham T. et ZELIKOWV, Philip, D., *Essence of Decision: Explaining the Cuban Missile Crisis*, 2ème édition, Longman, 1999.
- AMPERE André-Marie, *Essai sur la philosophie des sciences ou Exposition analytique d'une classification naturelle de toutes les connaissances humaines*, Paris, Bachelier, 1834, 654 p.
- ANDREWSKY Evelyne et DELORME Robert, *Seconde cybernétique et complexité - Rencontres avec Heinz von Foerster*, coll. Philosophie des sciences et techniques, L'Harmattan, Paris, juin 2006, 168 p.
- APTER Emily, *The Translation Zone*, Princeton, Princeton University Press, 2006, 225 p.
- ARCHIBUGI Danielle, et al., *Re-Imagining Political Community: Studies in Cosmopolitan Democracy*. Stanford University Press., 1998, 357 p.
- ARON Raymond (1962), *Paix et guerre entre les nations*, Paris, Calmann-Lévy, 20 janv. 2004, 832 p.
- ARSENE Séverine, *Internet et politique en Chine : les contours normatifs de la contestation*, Paris, Karthala, 2011, 420 p.
- ASHBY William Ross, *An Introduction to Cybernetics* (1957), Martino Fine Books, 25 janv. 2015, 306 p.

- ASIMOV Isaac, « Runaround », *Analog Science Fiction and Fact*, Mars 1942.
- AXELOS Kostas (1961), *Marx penseur de la technique*, Encre Marine, La Versanne, 2015, 464 p.
- AYRES Robert U., *Information, Entropy and Progress : A New Evolutionary Paradigm*, New York, American Institute of Physics, The AIP Press, 1994, 301 p.
- BACHELARD Gaston (1938), *La formation de l'esprit scientifique : contribution à une psychanalyse de la connaissance*, Paris, Vrin, 1993, p. 16.
- BARNES Harry Elmer (dir). *Perpetual War for Perpetual Peace: a Critical Examination of the Foreign Policy of Franklin Delano Roosevelt and Its Aftermath*. Caldwell, Caxton Printers, 1953, 500 p.
- BARTHES Roland, *Mythologies*, Paris, Éditions du Seuil, 1957 - 267 p.
- BASLE Maurice, *Approches évolutionnistes de la firme et de l'industrie: théories et analyses empiriques*, L'Harmattan, 1999, 367 p.
- BAUER, Harry et BRIGHI Elisabetta (dir.) *Pragmatism in International Relations*. New York, Routledge, 2009, 208 p.
- BEARD Charles (Macmillan, 1913), *An Economic Interpretation of the Constitution of the United States*, Courier Corporation, mars 2012, 336 p.
- BENIGER James R., *The Control Revolution Technological and Economic Origins of the Information Society*, Harvard University Press, 1986, 436 p.
- BERGER Peter et LUCKMANN Thomas, *La construction sociale de la réalité*, Paris, Armand Colin, 3ème édition, 2012, 344 p.
- BERNSTEIN Jay M. (1995), *Recovering Ethical Life : Jürgen Habermas and the Future of Critical Theory*, Londres, Routledge, 2014, 264 p.
- BERSINI Hugues, SPINETTE-ROSE Marie-Paule, SPINETTE-ROSE Robert, et VAN ZEEBROECK Nicolas (2008), *Les fondements de l'informatique : du bit au cloud*, 3ème édition, Paris, Vuibert, septembre 2014, 404 p.
- BIJKER Wiebe E, HUGHES Thomas P. et PINCH Trevor J. (eds.), *The social construction of Technological Systems*, Londres, MIT Press, 1987, 470 p.
- BONDITTI Phillippe, BIGO Didier et GROS Frédéric, *Foucault and the Modern International, Silences and Legacies for the Study of World Politics*, New York, Palgrave, 2017, 376 p.
- BOOTH Ken, *Theory of World Security*, Cambridge University Press, 2007, 516 p.

- BOURDIEU Pierre, CHAMBOREDON Jean-Claude, PASSERON Jean-Claude, *Le Métier de Sociologue*, Paris, École Pratique des Hautes Études, Mouton and Bordas, 1968, 432 p.
- BOURDIEU Pierre, « Décrire et prescrire. Les conditions de possibilités et les limites de l'action politique », In. BOURDIEU Pierre, *Ce que parler veut dire. L'économie des échanges linguistiques*, Paris, Fayard, 1982, pp. 149-161.
- BRETON Philippe, PROULX Serge, *L'explosion de la communication : la naissance d'une nouvelle idéologie*, Paris, La Découverte, 1993, 323 p.
- BRUNETEAU Bernard, *Les Totalitarismes*, Paris, Armand Colin, mai 2014, 320 p.
- BRYANT William D., *International Conflict and Cyberspace Superiority: Theory and Practice*, Routledge, 2016, 220 p.
- BULL Hedley, *Justice in International Relations*, University of Waterloo, Hagey Lectures, 1983.
- BUTTERFIELD Herbert et WIGHT Martin *Diplomatic investigations: Essays in the theory of international politics*, Crows Nest, Allen & Unwin, 1966, 227 p.
- BUZAN Barry & LITTLE Richard, *International Systems in World History: Remaking the Study of International Relations*, Oxford University Press, 2001, 476 p.
- BUZAN Barry, LITTLE Richard, et JONES Charles, *The Logic of Anarchy: Neorealism and Structural Realism*. New York, Columbia University Press, 1993, 267 p.
- BUZAN Barry, *The United States and the Great Powers: World Politics in the Twenty-First Century*, Cambridge, Polity, 2004, 240 p.
- BUZAN Barry, WÆVER Ole et WILDE (DE) Jaap, *Security : a New Framework for analysis* Lynne Rienner Publishers, 1998, 239 p
- ČAPEK Karel, *R.U.R. Reson's Universal Robots*, Paris, Editions de La Différence, février 2011, 220 p.
- CARR Edward H., *The Twenty Years' Crisis, 1919–1939: An Introduction to the Study of International Relations*, Londres, Macmillan, 1939, 312 p.
- CARR Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Londres: O'Reilly, 2009, 318 p.
- CASTELLS Manuel (1996), *L'Ère de l'information. Vol. 1, La Société en réseaux*, Paris, Fayard, 1998, 613 p.
- CASTELLS Manuel, *La Galaxie Internet*, Paris, Fayard, 2002, 365 p.

- CHAMONNOIS Suzanne et LABRIOLLE François, *L'Estonie : des Estes aux Estoniens*, Paris, Karthala (Méridiens), 1997, 277 p/
- CHARAUDEAU Patrick, *Langage et discours, Éléments de sémiolinguistique*, Paris, Hachette Université, Coll. Langue, Linguistique, Communication, 1983, 176 p.
- CHARAUDEAU Patrick, *Le discours politique. Les masques du pouvoir*, Paris, Vuibert, 2005, 256 p.
- CHATEAURAYNAUD Francis et TORYN Didier, *Les sombres précurseurs : une sociologie pragmatique de l'alerte et du risque*, Paris, EHESS, 1999, 476 p.
- CHAUMONT Jean-Michel, La concurrence des victimes : génocide, identité, reconnaissance, La Découverte, 1997, 392 p.
- CHEMOFF Fred, Theory and MÉtatheory in International Relations : Concepts and Contending Accounts, New York, Palgrave Macmillan, 2007, pp. 40-46.
- CHOMSKY Noam, Sur la nature et le langage, Éditions Agone, coll. « Banc d'essais », 2011, 224 p
- CHOMSKY Noam et FOUCAULT Michel, *Sur la nature humaine, comprendre le pouvoir, interlude*. Editions Aden, Bruxelles, octobre 2005, 200 p., (pp 7 – 87).
- CHOUCRI Nazli et Clark David D., *International Relations in the Cyber Age: The Co-Evolution Dilemma*, Cambridge, The MIT Press, 2019, 420 p.
- CHOUCRI Nazli. *Cyberpolitics in International Relations*. MIT Press, 2012, 320 p.
- CLARK Ian, *Globalization and International Relations Theory*. Oxford University Press, 1999, p. 1.
- CLARKE Richard A., et Knake Robert K., *Cyber War: the Next Threat to National Security and What to Do about It*. HarperCollins Publishers, 2010, 320 p.
- COOK Gary (dir.), *Clicking clean, who is winning race to build a green Internet?* Washington, Greenpeace, janvier 2017, 102 p.
- CORNUT Jérémie, *Les excuses dans la diplomatie américaine : Pour une approche pluraliste des relations internationales*, Montréal Les Presses de l'Université de Montréal, 2014, 189 p.
- COULOURBARITSIS Lambros « Chapitre 6. L'aristotélisme », In. *Aux origines de la philosophie européenne*, Bruxelles, De Boeck Supérieur, « Le Point philosophique », 2003 (4e éd.), p. 387-563.

- COX Robert W. et SINCLAIR Timothy J., *Approaches to World Order*, Cambridge, Cambridge University Press, 1996, 572 p.
- CROSS Mai'a K. Davis, *Security IngrÉation in Europe, How Knowledge-Based Networks Are Transforming the European Union*. Ann Arbor, University of Michigan Press, 2011. pp. 177 – 185.
- CROSS Mai'a K. Davis, *The European Diplomatic Corps: Diplomats and International Cooperation from Westphalia to Maastricht*, Londres, Palgrave Macmillan, 2007, 244 p.
- CROZIER Michel et FRIEDBERG Erhard, (1977). *L'acteur et le système : les contraintes de l'action collective*. Coll. « Points Essais ». Paris, Éditions du Seuil, 2014, 512 p.
- CROZIER Michel. *Le phénomène Bureaucratique : Essai Sur Les Tendances Bureaucratiques Des systèmes Dorganisation Modernes Et Sur Leurs Relations En France Avec Le systèmes Social Et Culturel*, Paris, Ed. Du Seuil, 1993, 413 p.
- CUDWORTH Erika et HOBDEN Stephen, *Posthuman International Relations: Complexity, Ecologism and Global Politics*, New York, Zed Books Ltd, avril 2013, 224 p.
- CUSSET François (2003), *French Theory. Foucault, Derrida, Deleuze & Cie et les mutations de la vie intellectuelle aux États-Unis*. Paris, Éditions La Découverte, 2005, 352 p.
- DAHL Robert, *Modern Political Analysis*, Englewood Cliff, Prentice Hall, 1963, p. 8,
- DENAT Céline, *Aristote*, Paris, Ellipses, 2010, 180 p.
- DERRIDA Jacques, *De la grammatologie*, Paris, Minuit, 1967, 448 p.
- DOBRY Michel (1987). *Sociologie des crises politiques*. La dynamique des mobilisations multisectoriellesn Paris, Presses de Sciences Po, 3ème édition, 2009, 432 p.
- DODGE Martin et KITCHIN Rob, *Mapping Cyberspace*, Routledge, 2003, 280 p.
- DODGE Martin, *The geographies of cyberspace*, 1999
- DOLPHIJN Rick, et TUIN (VAN DER) Iris, *New Materialism: Interviews & Cartographies*, Ann Arbor, Open Humanities Press, 2012, 200 p.
- DONOVAN James, A., *Militarism, U.S.A.* New York, Scribner, 1970, 265 p.
- DOSI Giovanni., NELSON R., Winter Sydney, *The nature and Dynamics Capabilities of the Firm*, Oxford, Oxford University Press, 2001, 408 p.

- DRUCKER Peter, F. (1969), *The Age of Discontinuity: Guidelines to Our Changing Society*, Transaction Publishers, déc. 2011, 420 p.
- DUPUY Gabriel, *Internet Géographie d'un réseau*, Paris, Ellipses, 2002, 160 p
- DURKHEIM Emile (1893), *De la division du travail social*, Paris, PUF, coll. Quadrige, 2007, 416 p.
- DURKHEIM Emile, *De la Division du travail social*, Librairie Félix Alcan, 1893, p. 173.
- ELIAS Norbert (1975) *La dynamique de l'occident*, Pocket, coll. Agora, 2003, 320 p.
- ELIAS Norbert *Qu'est-ce que la sociologie ?* Paris, Pocket, 1991.
- ELLUL Jacques (1977), *Le système technicien*, Paris, Calmann-Lévy, 2012, 396 p.
- FAINZANG Sylvie, *Ethnologie des anciens alcooliques*, Puf, 1998, 2e éd., 176 p.
- FAUCHEUX Michel, NORBERT Wiener, *le Golem et la cybernétique*, Paris, Editions du Sandre, Paris, 2008, 188 p.
- FAVRE Pierre, *Naissances de la Science Politique en France 1870-1914*, Paris, Fayard 1989, 331 p.
- FEENBERG Andrew, *Between Reason and Experience: Essays in Technology and Modernity*, MIT Press, 2010, 284 p.
- FEENBERG Andrew, *Transforming Technology a Critical Theory Revisited*. Oxford Univ. Press, 2002, 232 p.
- FLORIDI Luciano, *Internet: un exposé pour comprendre, un essai pour réfléchir*, Paris, Flammarion, 1998, 127 p.
- FLORIDI Luciano, *Philosophy and Computing: An Introduction*. Routledge, Londres / New York, 1999, 256p.
- FOUCAULT Michel (1969), *Archéologie du savoir*, Paris, Gallimard, 2014, 294 p.
- FOUCAULT Michel, *Les mots et les choses : une archéologie des sciences humaines*, Paris, Gallimard, 1966, 405 p.
- GALLOUEDEC-GENUYS Françoise, et MAISL Herbert, *Le Secret Des Fichiers*, Éditions Cujas, 1976, 328 p.
- GASTON-GRANGER Gilles, *Sciences et réalité*, Paris, Odile Jacob, 2001.
- GEORGE Éric et Granjon Fabien, *Critiques de la société de l'information*, Paris, L'Harmattan, 2008, 268 p.
- GHAMARI-TABRIZI Sharon, *The Worlds of Herman Kahn: The Intuitive Science of Thermonuclear War*, Harvard University Press, 2005, 432 p.

- GIBSON James William. *The Perfect War: Technowar in Vietnam*. Boston, Atlantic Monthly Press, 1986, 523 p.
- GIBSON William, *Neuromancer*, New-York, Ace books, juillet 1984, 271 p.
- GILLE Bertrand (dir.), *Histoire des techniques*, Paris, Gallimard, La pléiade, 1978, 1680 p.
- GODIN Benoît, *Innovation Contested – The Idea of Innovation Over the Centuries*. Londres, Routledge, 2015, 354 p.
- GRAY Chris Hables (2005). *Peace, War and Computers*. Londres, Routlege, 2013, 240 p.
- GRAY Chris Hables. *Postmodern War: the New Politics of Conflict*. New York, Guilford Press, 1997, 314 p.
- GUCHET Xavier, « L'objectivité technologique », Pour un humanisme technologique, Paris, PUF, « Pratiques théoriques », 2010, pp. 133-190.
- GUISNEL Jean, *Guerres dans le cyberspace, services secrets et Internet*, Paris, La découverte, coll. « Enquêtes », octobre 1995, 252 p..
- HAAS Peter M. *Saving the Mediterranean: The Politics of International Environmental Cooperation*, Columbia University Press, 1990, pp 17 – 25.
- HABERMAS Jürgen (1968), *La technique et la science comme « idéologie »*, trad. et préface par LADMIRAL Jean-René, Paris, Gallimard, 1973, 213 p.
- HABERMAS Jürgen (1968), *La Technique et la science comme « idéologie »*, Paris, Gallimard, 1990, 211 p.
- HABERMAS Jürgen (1981), *Théorie de l'agir communicationnel*, Volume 1, Rationalisé de l'agir et rationalisation de la société Paris, 1987, 448 p.
- HABERMAS Jürgen, *De l'éthique de la discussion*, Paris, Fayard 1999, 202 p.
- HABERMAS Jürgen, *La technique et la science comme « idéologie »*, Gallimard, 1990, 213 p.
- HACHMEITER Lutz, HEIDEGGERS *Testament. Der Philosoph, der Spiegel und die SS*, Propyläen, Berlin, 2014, 368 p.
- HALLIDAY Fred, *Rethinking International Relations*, Vancouver, University of British Columbia Press, 1994, 304 p.
- HALLSTEN Henrik, *Explanation and Deduction: A Defence of Deductive Chauvinism*. Coronet Books Inc, 2001, 165 p.

- HARAWAY Donna J. *Modest Witness Second Millennium: Femaleman Meets Oncomouse: Feminism and Technoscience*. Routledge, 1997, 361 p.
- HARAWAY Donna Simians, *Cyborgs and Women : The Reinvention of Nature*. New York, Routledge, 1991, 312 p.
- HARREL Yannick, *La cyberstratégie russe*, Nuvis, 2013, 245 p.
- HAUBEN Ronda et HAUBEN Micheal, *Netizens : on the history and impact of Usenet and the Internet*, Wiley-IEEE Computer Society Press, mai 1997, 361 p.
- HEIDEGGER Martin (1954), « La question de la technique », dans *Essais et conférences*, Paris, Gallimard, coll. « Tel », n° 52, 1980, pp. 9 - 48.
- HERRERA Geoffrey L. , Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change, New York, SUNY Press, septembre 2006, 275 p.
- HERZ, John H. Political Realism and Political Idealism: a Study in Theories and Realities. University of Chicago Press, 1951, 275 p.
 - HOLLIS Martin et SMITH Steve, Explaining and Understanding International Relations, Clarendon Press, 1990 226 p.
- HOLMES David, Virtual Politics: Identity and Community in Cyberspace, Londres, Thousand Oaks, 1997, 256 p.
- HOLZNER Burkart, *Reality Construction in Society*. Cambridge: Mass., Schenkman Pub. Co 1968, 192 p ;
- HOLZNER Burkart and MARX John H., *Knowledge Application: The Knowledge System in Society*, Boston, Allyn & Bacon, 1979, pp. 107–111
- HORKHEIMER Max et ADORNO Theodor W. (1947), La Dialectique De La Raison: Fragments Philosophiques. Gallimard, 1974, 281 p.
- HORKHEIMER Max, *Critical Theroy : Selected Essays*, New York, Seabury Press, 1972, p. 208.
- HORKHEIMER Max, *Théorie traditionnelle et Théorie critique*, Paris, Gallimard, 324 p.
- HUGHES Thomas P , *Networks of Power: Electrification in Western Society, 1880-1930* , Baltimore, Johns Hopkins University Press, 1983, 476 p.
- HUITEMA Christian, *Et Dieu créa l'Internet*, Paris, Eyrolles, 1995, 201 p.
- HUYGHE François-Bernard, *L'ennemi à l'ère numérique, chaos, information, domination*, Paris, PUF, Coll. Défense et défis nouveaux, 2001, 216 p.

- INNIS, Harold A. (1951), *The Bias of Communication*, University of Toronto Press, 1977, 226 p.
- JAMESON Fredric, (1984), *Postmodernism, or the Cultural Logic of Capitalism*. Durham, Duke University Press, 1984, 438 p.
- JOHNSON Deborah G., *Computer ethics*. Prentice-Hall, Englewood Cliffs, 1985, 110 p.
- JORDAN Tim. *Cyberpower: the Culture and Politics of Cyberspace and the Internet*, Londres, Routledge, 1999, 248 p.
- KALDOR, Mary. *The Imaginary War : Understanding the East-West Conflict*. Cambridge, Basil Blackwell, 1990, 298 p.
- KALINOWSKI Isabelle, *La science, profession et vocation. Suivi de "Leçons webériennes sur la science & la propagande"*, Paris, Agone, 2005, 300 p.
- KALYVAS Andréas Democracy and the Politics of the Extraordinary: Max Weber, Carl Schmitt, and Hannah Arendt. Cambridge: Cambridge University Press, 2008, 340 p.
- KAPLAN Fred (1983), *The Wizards of Armageddon*, Stanford University Press, août 1991, 452 p. ;
- KECK Margaret E, et SIKKINK Katheryn, *Activists beyond Borders: Advocacy Networks in International Politics*, Ithaca, Cornell University Press, 1999, 240 p
- KEOHANE Robert O. et NYE Joseph S., *Power and Interdependence: World Politics in Transition*, Little, Brown and Company, 1977, 273 p.
- KEOHANE, Robert Owen et NYE Joseph S., Power and Interdependence, New York, Harper Collins.1989.
- KEOHANE, Robert Owen et NYE Joseph S., Power and Interdependence: World Politics in Transition. Boston, Little, Brown, 1977, 273 p.
- KING Gary, KEOHANE Robert O. et SIDNEY Verba, *Designing Social Inquiry: Scientific Inference in Qualitative Research*, Princeton University Press, 1994,
- KLARE Michael T., *War Without End: American Planning for the Next Vietnam*, New York, Knopf, décembre 1972, 464 p.
- KRAMER, Franklin D., et al. (dir), *Cyberpower and National Security*. Center for Technology and National Security Policy, 2009, 664 p.
- KRIEG-PLANQUE Alice, *Analyser les discours institutionnels*, Paris, Armand Colin, 2012, pp. 155-185.

- KUHN Thomas, *La Structure des révolutions scientifiques*, Paris, Flammarion, coll. « Champs-Sciences », 2008, 286 p.
- KURKI Milja, *Causation in International Relations: Reclaiming Causal Analysis*, Cambridge Studies in International Relations, Cambridge University Press, avril 2008, 370 p.
- KURKI Milja, *Causation in International Relations: Reclaiming Causal Analysis*, Cambridge University Press, 2008, 309 p.
- LAFFITE Jacques, *Réflexions sur la science des machines*, Paris, Vrin, 1972, 136 p.
- LAFONTAINE Cécile, *L'Empire cybernétique. Des machines à penser à la pensée machine*, PARIS, SEUIL, 2004, 240 p. ;
- LAGROYE Jacques, « Les processus de politisation », In. Lagroye Jacques (dir.), *La politisation*, Paris, Belin, 2003, p. 359-372
- LALLEMENT Michel, *L'Âge du faire. Hacking, travail, anarchie*, Paris, Seuil, 2015, 442 p.
- LATOUR Bruno *Science in Action: How to Follow Scientists and Engineers through Society*, Harvard University Press, 1987, 274 p.
- LATOUR BRUNO, et Woolgar Steve. *La Vie De Laboratoire La Production Des Faits Scientifiques*. Paris, Editions La Découverte, 1979, 271 p.
- LATOUR BRUNO, *Les Microbes: Guerre Et Paix ; Suivi De: Irréductions*. A.M. Métailié, 1984, 281 p.
- LASSWELL Harold D., *Politics: Who Gets What, When, How*, New York, Meridian Books, 1958, 222 p.
- LEBRETON David, *L'adieu au corps*, Coll. Traversées, Métailié, 1999, 237 p.
- LEROI-GOURHAN André, *Le geste et la parole, Volume 1*, Paris, A. Michel, novembre 1964, 326 p.
- LESSIG, Lawrence, *Code and Other Laws of Cyberspace*. Basic Books, 1999, 320 p.
- LESSIG Lawrence, *The Future of Ideas: the Fate of the Commons in a Connected World*. Random House, 2001, 297 p.
- Lévy Jacques et LUSSAULT Michel, *Dictionnaire de la géographie de l'espace des sociétés*, Paris, Belin, 1033 p.
- LIBICKI Martin C., *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press, 2007, 336 p.

- LINKLATER Andrew, *Men and Citizens in the Theory of International Relations*, Springer, 1982, 232 p.
- LINKLATER Andrew, *The Problem of Harm in World Politics: Theoretical Investigations*, Cambridge University Press, 2011, 306 p.
- LOVELUCK Benjamin, *Réseaux, libertés et contrôle : Une généalogie politique d'internet*, Paris, Armand Colin, 21 oct. 2015, 368 p.
- LYOTARD Jean-François, *Le Postmoderne expliqué Aux Enfants: Correspondance, 1982-1985*. Galilée, 1986, 165 p.
- MACIVER Robert M., *Community*, Londres, Macmillan, 1924, 446 p.
- MACKENZIE Donald A. *Inventing Accuracy: a Historical Sociology of Nuclear Missile Guidance*. MIT Press, 2001, 478 p
- MARCUSE Herbert (1964), *L'Homme unidimensionnel*, Paris, Editions de Minuit, 1968, 281 p.
- MARKUS Gyorgy, *Langage et production*, Paris, Denoël, 1982, 222 p.
- MASCO Joseph P. *The Nuclear Borderlands: The Manhattan Project in Post-Cold War New Mexico*, Paperback, janvier 2006, 448 p.
- MATTELART Armand (2001), *Histoire de la société de l'information*, Paris, 4ème édition, La Découverte, juillet 2010, 128 p
- MAUSS Marcel, *Œuvres, Tome III. Cohésion sociale et division de la sociologie*, Paris, Les Éditions de Minuit, coll. Le sens commun, 1969, pp. 626-634.
- McCARTHY Daniel R., *Power, Information Technology, and International Relations Theory: the Power and Politics of US Foreign Policy and the Internet*. Palgrave Macmillan, 2015, 220 p.
- MCRAE, Ronald M., *Mind Wars: the True Story of Government Research into the Military Potential of Psychic Weapons*. New York, St. Martins Press, 1984, 155 p.
- MCSWEENEY Bill, *Security, Identity and Interests. A Sociology of International Relations*, Cambridge, Cambridge University Press, 1999, p 203.
- MEIKLE Graham (dir.), *The Routledge Companion to Media and Activism*, New York, Routledge, mars 2018, 420
- MELMAN, Seymour. *The Permanent War Economy; American Capitalism in Decline*. New York, Simon and Schuster, 1974, 384 p.

- MOATI Raoul, Derrida, *Searle : Déconstruction et langage ordinaire*, Paris, PUF, coll. Philosophies, 2009, 153 p.
- MORIN EDGAR, *Introduction à la pensée complexe*, Paris, Seuil, coll. « Points / Essais », 2005, 158 p.
- MOSCOVICI Serge, *La Psychanalyse, son image et son public*, Paris, PUF, 1961. 512 p.
- MUMFORD Lewis (1967) *le Mythe de la machine, Tome 1 : La Technologie et le développement humain*, Paris, Fayard, 1974.
- MUMFORD Lewis (1970) *le Mythe de la machine, Tome 2 : Le Pentagone de la puissance*, Paris, Fayard, 1974.
- NEGROPONTE Nicholas, *L'homme numérique*, Paris, Robert Laffont, avril 1995, 290 p.
- NEUFELD Mark, *The Restructuring of International Relations Theory*, Cambridge, Cambridge university Press, 1995, 174 p.
- NEUMANN (von) John (1958), *L'Ordinateur et le cerveau* Flammarion, 1999, 125 p.
- NEVEU Éric, *Une société de communication ?*, Montchrestien, 2011, 160 p.
- NEWMAN, Abraham L, *Protectors of Privacy: Regulating Personal Data in the Global Economy*, Ithaca, Cornell University Press, juillet. 2018, 240 p.
- NISBET Robert A., *History of the Idea of Progress*, Transaction Publishers, 1980, 370 p.
- NORA Dominique (1995), *Les Conquérants du cybermonde*, Paris, Calmann-Lévy, avril 2014, 355 p.
- NORTH Douglass C., *Institutions, Institutional Change and Economic Performance*. Cambridge University Press, 1990, 152 p.
- NYE Joseph S. *Soft Power: The Means To Success In World Politics*, Hachette UK, 28 avr. 2009 - 208 p.
- NYE Joseph S., *The future of power*, New York, PublicAffairs, 2011, 320 p. ;
- NYSTRAND Martin, *The structure of written communication: Studies in reciprocity between writers and readers*. Orlando, FL: Academic, 1986, 234 p.
- ONUF Nicholas (1982), *World of our Making : Rules and Rule in Social Theory and International Relations*, Routledge, 2012, 340 p.
- OTMAN Gabriel, *Les mots de la cyberspace*, Belin, 1998, 474 p.
- PARRY Richard, « Episteme and Techne », In. Collectif, *The Stanford Encyclopedia of Philosophy*, The Metaphysics Research Lab, Standford, septembre 2014.

- PASSERON Jean-Claude, *Le Raisonnement sociologique, l'espace non-poppérien du raisonnement naturel*, coll. Essais & recherches, Nathan, 1991, 408 p.
- PETERSON John et BOMBERG Elizabeth, *Decision-Making in the European Union*, Londres, Macmillan International, 1999, 352 p.
- PFEFFER Jeffrey et SALANCIK Gerald, *The External Control of Organizations*, New York, Harper & Row, 1978, 300 p.
- PLATON, *La République, livre VI*, Collection des universités de France, les Belles Lettres, 1932, § 488a - 490b
- POHL Frederick Julius. *The Cool War*. Corgi, 1983, 288 p.
- POPPER Karl (1963), *Conjectures et réfutations : la croissance du savoir scientifique*, Payot, 2006, 610 p.
- POSSONY Stefan Thomas et POURNELLE Jerry, *The Strategy of Technology; Winning the Decisive War*. University Press of Cambridge, 1970, 189 p.
- PROTEVI, John, *Life, War, Earth: Deleuze and the Sciences*. University of Minnesota Press, 2013, 264 p
- RADAELLI Claudio M., (1998), *Technocracy in the European Union*, Londres, Routledge, 2017, 184 p.
- RHEINGOLD Howard (1993),, *The Virtual Community: Homesteading on the Electronic Frontier*, MIT Press, octobre 2000, 480 p.
- RHEINGOLD Howard, *Tools for Thought: The History and Future of Mind-expanding Technology*, MIT Press, 1985, 359 p.
- RHEINGOLD Howard, *Virtual reality*, Secker & Warburg, 1991, 415 p.
- RICŒUR Paul, *Du texte à l'action, Essais d'herméneutique II*, Paris, Seuil, 1996, 416 p.
- RIFKIN Jeremy, *Time Wars: The Primary Conflict in Human History*, New York, Simon & Schuster, juin 1987. 302 p.
- RIORTY Richard (1967), *The Linguistic Turn. Recent Essays in Philosophical Method*, The University of Chicago Press, 1992, 416 p.
- RIST Gilbert, (1996) *Le développement : histoire d'une croyance occidentale*, Paris, Presses de Sciences Po, coll. « Monde et sociétés », 4e édition, 2013, 520 p.
- ROBERT Pascal, *L'impensé informatique: critique du mode d'existence idéologique des technologies de l'information et de la communication*, Volume 1, Archives contemporaines, 2012, 234 pages.

- ROE Emery, *Narrative Policy Analysis: Theory and Practice*, Duke University Press, 1994, 199 p.
- ROGERS, Everett M. (1962) *Diffusion of Innovations*. Free Press, 1995, 512 p.
- ROSENAU James N. *Turbulence in World Politics: a Theory of Change and Continuity*. Princeton University Press, 1990. 480 p.
- ROSENBERG Nathan , *Exploring the Black Box: Technology, Economics, and History*, Cambridge University Press, 1994, 274 p.
- ROSNAY (DE) Joël, *L'homme symbiotique : regards sur le troisième millénaire*, Paris, Seuil, 1995, 349 p.
- RUPERT Mark. *Producing Hegemony: the Politics of Mass Production and American Global Power*. Cambridge University Press, 1995, 280 p.
- SAKR Naomi. *Arab Television Today*. I.B.Tauris, 2007, 256 p.
- SAKR Naomi. *Satellite Realms Transnational Television, Globalization and the Middle East*. I.B. Tauris, 2001, 280 p.
- SAMAAN Jean-Loup, *La RAND Corporation (1989-2009): La reconfiguration des savoirs stratégiques aux États-Unis*, Paris, l'Harmattan, 2010, 252 p.
- SCHAFER Valérie, *La France en réseaux: Tome 1, La rencontre des télécommunications et de l'informatique (1960-1980)*, Vol. 1, Paris, Nuvis, 2012, 384 p.
- SCHELL Bernadette H., et CLEMENS Martin. Cybercrime: a Reference Handbook. ABC-CLIO, octobre 2004, 247 p.
- SCHLANGER Nathan, « Une technologie engagée : Marcel Mauss et l'étude des techniques en sciences sociales » In.. SCHLANGER Nathan, *Marcel Mauss, Techniques, technologie et civilisation*, Paris, PUF, coll. Quadrige, septembre 2012, pp 17-134
- SCHMIDT Brian C. , *International Relations and the First Great Debate*, Londres, Routledge, 2012, 192 p.
- SCHMIDT Brian C. (1998), *Political Discourse of Anarchy, The: A Disciplinary History of International Relations*, New York, SUNY Press, 2016, 309 p.
- SCHRECKER Cherry, *La Communauté. Histoire critique d'un concept dans la sociologie anglo-saxonne*, Paris, L'Harmattan, 2006, 283 p.
- SCHWARTAU Winn (1994), *Information Warfare: Chaos on the Electronic Superhighway*, Thunder's Mouth Press, 1995, 432 p.
- SEARLE John R. *The Construction of Social Reality*, Simon and Schuster, 1995, 241 p.

- SEGAL Jérôme, *Le Zéro et le Un : histoire de la notion scientifique d'information au 20e siècle*, Syllepse, 2003, 890 p.
- SFEZ Lucien, *Technique et idéologie. Un enjeu de pouvoir*, Paris, Le Seuil, 2002, 336 p.
- SHACKELFORD, Scott J.. *Managing Cyber Attacks in International Law, Business, and Relations: in Search of Cyber Peace*. Cambridge Univ Press, 2016, 434 p.
- SHANNON Claude, E. et WEAVER, Warren, *The Mathematical Theory of Communication* (1934), University of Illinois Press, 1963, 125 p.
- SIL Rudra et KATZENSTEIN Peter J., *Beyond Paradigms: Analytic Eclecticism in the Study of World Politics*, Macmillan, 2010, 240 p.
- SIMONDON Gilbert (1958), *Du mode d'existence des objets techniques*, Aubier, 2012, 367 p.
- SKINNER Quentin (1981), *Machiavel*, Paris, Le Seuil, coll. « Philosophie Générale », 1989, 181 p.
- SMITH Bruce (1966), *The RAND Corporation: Case Study of a Nonprofit Advisory Corporation*, Harvard University Press, 2013, 348 p.
- SNYDER Richard C., BRUCK Henry W. et SAPIN Burton M. (dir), (1954), *Foreign Policy Decision Making: An Approach to the Study of International Politics*, Literary Licensing, LLC, 2012, 286 p.
- STERLING Bruce (ed.) *Mirrorshades: The Cyberpunk Anthology*, Arbor House, 1986, 320 p.
- SUCHMAN Lucy, A. *Plans and situated actions: The problem of human-machine communication*. Cambridge university press, 1987.
- SUN Tzu, « I – De l'évaluation » in. *L'Art de la Guerre*, Paris, Éditions Flammarion, collection « Champs », 1978.
- SUSSAN Remi, *Les utopies posthumaines: contre-culture, cyberculture, culture du chaos*, Omniscience, coll. Les essais, 2005, 287 p.
- SWALES, John M. *Genre Analysis: English in Academic and Research Settings*. Cambridge, Cambridge University Press, 1990, 286 p.
- TAGUIEFF Pierre-Alexandre, L'idée de progrès une approche historique et philosophique (2004), coll. Champs/essais, Flammarion, 2011, 445 p.

- TAILLAT Stéphane, CATTARUZZA Amaël et DANET Didier (dir.), *La Cyberdéfense - Politique de l'espace numérique*, Paris, Armand Collin, juillet 2018, 357 p.
- TARDE Gabriel, *les lois de l'imitation*, Paris, F. Alcan, 1890, 431 p.
- TARDE Gabriel, *Les transformations du droit*. Étude sociologique (1891), Paris, Berg International Éditeurs, 2e édition, 1994, 216 p.
- TARDE Gabriel, *Les transformations du droit. Étude sociologique*, (mai 1891), 2e édition, Paris, Berg International Éditeurs, 1994, 216 pp.
- TENEZE Nicolas, *Combattre les cyberagressions*, Paris, Nuvis, Janvier 2018, 578 p.
- TESCHKE Benno, *The Myth of 1648: Class, Geopolitics and the Making of Modern International Relations*, Londres, Venno, 2003, 308 p.
- TOFFLER Alvin, et Toffler Heidi. *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston, Little, Brown & Co, 1993, 302 p.
- TOFFLER Alvin, *La troisième vague*, Paris, Folio, coll. Essais, 1980, 635 p.
- TÖNNIES Ferdinand (1887), *Communauté et société : catégories fondamentales de la sociologie pure*, Paris, PUF, sept. 2015, 336 p.
- TRICLOT Mathieu, *Le Moment cybernétique, la constitution de la notion d'information*, Champ Vallon, 2008, 422 p.
- VALERIANO Brandon, et MANESS Ryan C., *Russia's Coercive Diplomacy : Energy, Cyber, and Maritime Policy as New Sources of Power*, Londres, Palgrave Macmillan, 2015, 250 p.
- VAN CREVELD Martin, *Technology and War: From 2000 B.C. to the Present*, Washington, D.C, Free Press, 1989, 342 p.
- VAN DER PIJL Kees, (1984) *The Making of an Atlantic Ruling Class*, Verso Books, 2012, 331 p.
- VANDENDORPE Christian, *Du papyrus à l'hypertexte*, Boréal, Montréal, La découverte, Paris, 1999, p. 31
- VASSILIOU Marius, ALBERTS David S., et AGRE Jonathan R, *C2 Re-Envisioned: the Future of the Enterprise*, CRC Press, New York, déc. 2014, 316 p.
- VENTRE Daniel , *Cyberespace et acteurs du cyberconflict*. Hermès Publishing. Paris, 2011, p. 13
- VENTRE Daniel, *Cyberattaque et cyberdéfense*, Paris, Hermes Lavoisier, 2011, 312 p.

- VERNADSKY Vladimir .I., *Biosphera (The Biosphere)*, Scientific Chemico-Technical Publishing: Leningrad, 1926, 200 p.
- VIRILIO Paul et LOTRINGE, Sylvère, *Pure war. New York*, Semiotext(e), 1983, 174 p.
- VIRILIO Paul et LOTRINGER Sylvère *Pure war : twenty-five years later*, Los Angeles, MIT Press, 2008, 253 p.
- VIRILIO Paul, *Vitesse et Politique*, Paris, Galilée, 1977, 151 p.
- WALTZ Kenneth, *Theory of International Politics*, McGraw-Hill, janvier 1979, 251 p.
- WALTZ Kenneth (1959), *Man, the State, and War*, Columbia University Press, 2001, 263 p.
- WARUSFEL, Bertrand. *Contre-Espionnage Et Protection Du Secret: Histoire, Droit Et Organisation De La sécurité Nationale En France*. Parisn Lavauzelle, 2000, 496 p.
- WEBER Max (1921), *Economie et société, tome 1 : Les Catégories de la sociologie*, Paris, Pocket, janvier 2003, 410 p.
- Weber Max (1959), *Le savant et le politique*, La découverte, 2003, 206 p.
- WELLS Herbert George (1895), *La Machine à explorer le temps*, Chapitre VI, Le Crépuscule de l'humanité, Paris, Larousse, 2017, p. 47.
- WENDT Alexander, *Social Theory of International Politics*, Cambridge University Press, 1999, 429 p.
- WENDT, Alexander. *Quantum Mind and Social Science Unifying Physical and Social Ontology*, Cambridge University Press, 2015, 366 p.
- WENGER Etienne, *Communities of Practice: Learning, Meaning, and Identity*, Cambridge University Press, 1999, 318 p.
- WESTRUM Ron. *Technologies & Society: The Shaping of People and Things*. Belmont, Wadsworth Pub. Co, 1991, 394 p.
- WIENER Norbert, *Cybernétique et société, l'usage humain des êtres humains*, Paris, UGE, coll. « 10/18 », 1954, 248 p.
- WIGHT Martin, *International Theory: The Three Traditions*, Holmes & Meier, 1991, 286 p.
- WILCOX Lauren B. *Bodies of Violence: Theorizing Embodied Subjects in International Relations*. Oxford University Press, 2015, 252 p.
- WINTER Sydney, *An Evolutionary Theory of Economic Change*. Cambridge, Belknap Press/Harvard University Press, 1982. 400 p.

- WYN Jones Richard, *Security, Strategy, and Critical Theory*, Lynne Rienner Publishers, 1999, 191 p.
- ZETLAOUI Tiphaine (dir.), *Histoire(s) de l'Internet*, Paris, L'Harmattan, avril 2015, 226 p.

Thèses

- CORNUT Jérémie, *Le pragmatisme et l'analyse des phénomènes complexes dans la théorie des relations internationales : le cas des excuses dans la diplomatie américaine*, thèse de Science Politique, dirigée par Battistella Dario et Roussel Stéphane, soutenue en 2012, 329 p.
- DESFORGES Alix, *Approche géopolitique du cyberspace, enjeux pour la défense et la sécurité nationale, l'exemple de la France*, soutenue le 27 août 2018 à l'Institut français de Géopolitique, Université Paris 8 Vincennes/Saint-Denis, sous la direction de Frédéric Douzet, 398 p
- LEDEVEDEC Nicolas, *La société de l'amélioration : du renversement de la perfectibilité humaine, du l'humanisme des lumières à l'humain augmenté*, thèse de science politique sous la direction de Céline Lafontaine et Jean Baudouin, Université de Montréal / Université de Rennes 1, soutenue en septembre 2013 (non publiée au moment de la rédaction).
- SERRES Alexandre, *l'émergence d'ARPANET. Exploration du processus d'émergence d'une infrastructure informationnelle. Description des trajectoires des acteurs et actants, des filières et des réseaux constitutifs de la naissance d'ARPANET. Problèmes critiques et épistémologiques posés par l'histoire des innovations*, Thèse de doctorat en science de l'information et de la communication, Université Rennes 2, soutenue en octobre 2000, 590 p.

Articles de revue

- AUGE Axel, « La formation initiale des futures élites militaires à Saint-Cyr : un dispositif institutionnel en évolution », *Education et sociétés*, 2008/1 (n° 21), p. 81-94.
- ABBEY Ruth et HYDE, Sarah, « No country for older people? Age and the digital divide », *Journal of Information, Communication and Ethics in Society*, Vol. 7 No. 4, 2009, pp. 225-242.

- ADLER Emanuel et HAAS Peter M., « Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program », *International Organization*, vol. 46, no. 1, 1992, pp. 367-390.
- ADLER Emanuel. « The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control. » *International Organization*, vol. 46, no. 1, 1992, pp. 101–145
- AKRICH Madeleine, « Comment décrire des objets techniques », *Techniques et Culture*, n°9, 1987, pp. 49-64.
- AKRICH Madeleine, « From Communities of Practice to Epistemic Communities: Health Mobilizations on the Internet », *Sociological Research Online*, vol. 15, no. 2, 2010, pp. 1–17;
- ALAM Thomas, GURRUCHAGA Marion, O'MIEL Julien, « Science de la science de l'État : la perturbation du chercheur embarqué comme impensé épistémologique », *Sociétés contemporaines*, 2012/3 (n° 87), p. 155-173.
- ALDEN Chris. « Let them eat cyberspace: Africa, the G8 and the digital divide. » *Millennium* vol. 32, n°3, 2003 : pp. 457-476.
- ALDER Emanuel et Pouliot Vincent, « International Practices », *International Theory*, n°3 (1), 2011, pp.1- 36.
- ARQUILLA John, et RONFELDT David. « Cyberwar Is Coming! » *Comparative Strategy*, vol. 12, no. 2, 1993, pp. 141–165.
- ASHLEY Richard K. « Untying the Sovereign State : A Double Reading of the Anarchy Problematique », *Millennium*, Vol 17, Issue 2, 1998, pp. 227 – 262.
- AUFRRET Yves, "Le vol numérique en question", *Journal Spécial des Sociétés*, n°62/2015, 30 décembre 2015.
- AUFRRET Yves, « Existe-t-il un marché des cyber-armes ? Pour une approche critique de la notion de cyber-arme », *Penser les ailes françaises*, n°35, juillet 2015, pp 103-111.
- AZUMA Ronald T., « A survey of Augmented reality », *Presence: Teleoperators and Virtual Environments* vol. 6, n°4, août 1997, pp 355-385.
- BAKIS Henry, « Le « géocyberespace » revisité », *Netcom*, 21-3/4, 2007, pp. 285-296.
- BALDWIN David, « The Concept of Security », *Review of International Studies*, vol. 23, n°1, 1997, pp. 5-26.

- BALZACQ Thierry, « The Three Faces of Securitization: Political Agency, Audience and Context », *European Journal of International Relations*, vol. 11, 2005, pp. 171 – 201.
- BALZACQ Thierry. « Théories de la sécurisation, 1989-2018. » *Études internationales*, volume 49, numéro 1, hiver 2018, pp. 7–24.
- BARBAROUX Pierre, « Cyberdéfense et cybersécurité du milieu aérospatial : quelles spécificités ? quelles ambitions ? », *Penser les ailles françaises*, n°32, juillet 2015 pp. 89 – 96.
- BARBAROUX Pierre, « Innovation disruptive et naissance d'un écosystème : voyage aux origines de l'internet », *Revue d'économie industrielle*, 2/2014 (n° 146), p. 27-59.
- BARDIES Laure, « Du concept de spécificité militaire », *L'Année sociologique*, 2011/2 (Vol. 61), p. 273-295.
- BARDINI Thierry et Proulx Serge, « La culture du hack en ligne, une rupture avec les normes de modernité », *Les Cahiers du numérique*, 2002, pp. 35-54.
- BARRY Anndrew, « The Translation Zone: Between Actor-Network Theory and International Relations », *Millennium*:; vol. 41 n°3, 2012, pp. 413-429.
- BARTHES Roland, « L'effet de réel ». In. *Communications*, « Recherches sémiologiques le vraisemblable »..11, 1968, pp. 84-89
- BAUD Michel, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique étrangère*, no. 2, été 2012, pp. 305-316.
- BAUD Michel. « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique étrangère*, vol. été, no. 2, 2012, pp. 305-316.
- BAUDOT Pierre-Yves, « L'incertitude des instruments. L'informatique administrative et le changement dans l'action publique (1966-1975) », *Revue française de science politique*, Vol. 61, 2011/1, pp. 79-103.
- BAUDOT Pierre-Yves. « L'incertitude des instruments. L'informatique administrative et le changement dans l'action publique (1966-1975) », *Revue française de science politique*, vol. vol. 61, no. 1, 2011, pp. 79-103.
- BEAU Francis, « Culture du renseignement et théories de la connaissance », *Revue internationale d'intelligence économique*, vol 2, no. 1, 2010, pp. 161-190.
- BELLAIS Renaud. « Les enjeux de la maîtrise de l'information dans la défense. » *Réseaux*, volume 16, n°91, 1998. *Les relations clients-fournisseurs à l'épreuve des réseaux*. pp. 121-133.

- BELLON, Anne. « Le hacker et le professeur. Mise en débat de la propriété intellectuelle sur Internet aux États-Unis », *Raisons politiques*, vol. 67, no. 3, 2017, pp. 165-183.
- BENIGER James R., « Information Society and Global Science », *The ANNALS of the American Academy of Political and Social Science*, 495(1), 1988 pp. 14–28.
- BERNSTEIN Richard, « Pragmatism, Pluralism and the Healing of Wounds », *Proceedings and Addresses of the American Philosophical Association*, Vol. 63, No. 3, Nov., 1989, pp. 5-18
- BETZ David J. et STEVENS Tim. « Analogical Reasoning and Cyber Security. » *Security Dialogue*, vol. 44, no. 2, 2013, pp. 147–164.
- BIGO Didier, « Sécurité et immigration : vers une gouvernementalité par l'inquiétude ? », *Cultures & Conflits*, 31-32, printemps-été 1998.
- BIMBER, Bruce. « Karl Marx and the Three Faces of Technological Determinism », *Social Studies of Science*, vol. 20, no. 2, 1990, pp. 333–351. ;
- BOËNE Bernard, « La formation initiale et sa place dans le continuum de la formation des officiers de carrière », *Stratégique*, 2017/3 (N° 116), p. 37-60.
- BOOTH Ken. « Security and Emancipation. » *Review of International Studies*, vol. 17, no. 4, 1991, pp. 313–326.
- BOURBEAU Philippe, « Politisation et sécurisation des migrations internationales : une relation à définir », *Critique internationale*, n° 61, 2013/4, pp. 127-145.
- BOURDIEU Pierre , « Espace social et genèse des classes », *Actes de la recherche en sciences sociales*, vol 52, 1984, p. 3-14.
- BOURDIEU Pierre. « Les conditions sociales de la circulation internationale des idées ». *Actes de la recherche en sciences sociales*. Vol. 145, « La circulation internationale des idées », décembre 2002. pp. 3-8.
- BOUSQUET Antoine « Chaoplexic Warfare or the Future of Military Organization, », *International Affairs*, vol. 84 n° 5, 2008, pp. 915-929.
- BOUTHERIN Grégory, « Un nouveau combat pour les UAV ? Quand les drones armés affrontent les perceptions », *Sécurité globale*, n°14, 2010, p. 111-124.
- BRAUN Benjamin, SCHINDLER Sebastian et WILLE Tobias, « Rethinking agency in International Relations: performativity, performances and actor-networks. », *Journal of International Relations and Development*, février 2018, pp. 1-21.

- BRONDIZIO Eduardo S., OSTROM Elinor et Young Oran R, « Connectivité et gouvernance des systèmes socio-écologiques multiniveaux : le rôle du capital social », *Management & Avenir*, n° 67, juillet 2013, pp. 108-140.
- BROWN Chris. « Cosmopolitanism, World Citizenship and Global Civil Society. » *Critical Review of International Social and Political Philosophy*, vol. 3, no. 1, 2000, pp. 7–26.
- BULINGE Franck, et Boutin Éric. « Le renseignement comme objet de recherche en SHS : le rôle central des SIC », *Communication & Organisation*, vol. 47, no. 1, 2015, pp. 179-195.
- BUZAN Barry, et WÆVER Ole « Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory. » *Review of International Studies*, vol. 35, no. 2, 2009, pp. 253–276
- CALLON Michel, « La domestication des coquilles Saint-Jacques et des marins-pêcheurs dans la baie de Saint-Brieuc », *L'année sociologique*, n°36, 1986, pp. 169-208 ;
- CALLON Michel, et FERRARY Michel. « Les réseaux sociaux à l'aune de la théorie de l'acteur-réseau », *Sociologies pratiques*, vol. 13, n°2, 2006, p. 41.
- CARR Madeline, « Public-private Partnerships in National Cyber-Security Strategies » *International Affairs*, vol. 92 n°1, pp. 43–62.
- DUNN CAVELTY Myriam et EGLOFF Florian J. , « The Politics of Cybersecurity: Balancing Different Roles of the State. », *St Antony's International Review* vol. 15 no.1 , 2019, pp. 37-57.
- DUNN CAVELTY Myriam, « Cybersecurity Research Meets Science and Technology Studies », *Politics and Governance*, Volume 6, Issue 2, juin 2018, pp. 22-30.
- DUNN CAVELTY Myriam. « Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. » *Science and Engineering Ethics*, vol. 20, no. 3, 2014, pp. 701–715.
- CEBROWSKI, Arthur K. et GARSTKA John J., « Network-Centric Warfare: Its Origins and Future, » *U.S. Naval Institute Proceedings*, Annapolis, Maryland, Janvier 1998.
- CERF Vinton G. et Kahn Robert E., « A protocol for packet network interconnection », *IEEE Trans. Comm . Tech. ,* vol. COM-22, V 5, mai 1974, pp. 627-641.
- CHALVIN Antoine, « L'ombre du soldat de bronze », *Le Courrier des pays de l'Est*, 2007/4 (n° 1062).

- CHARAUDEAU Patrick, « Le chercheur et l'engagement. Une affaire de contrat », *Argumentation et Analyse du Discours*, 11, octobre 2013, pp. 1-14.
- CHILSTEIN David. « Législation sur la cybercriminalité en France », *Revue internationale de droit comparé*, Vol. 62 N°2,2010. pp. 553-606.
- CHINN Menzie D. et FAIRLIE Robert W, « The Determinants of the Global Digital Divide: A Cross-Country Analysis of Computer and Internet Penetration. », *Oxford Economic Papers*, vol. 59 n°1, 2007, pp. 16–44.
- CHOUCRI Nazli. « Introduction: CyberPolitics in International Relations. », *International Political Science Review*, vol. 21, no. 3, 2000, pp. 243–263
- COCKBURN Cynthia, « The Material of Male Power » *Feminist Review*, n° 9, 1981, pp. 41-58.
- COHENDET Patrick, CREPLET Frédéric, et DUPOUËT Olivier. « Innovation organisationnelle, communautés de pratique et communautés épistémiques : le cas de Linux », *Revue française de gestion*, vol. no 146, no. 5, 2003, pp. 99-121.
- COMOR Edward, « The Role of Communication in Global Civil Society: Forces, Processes, Prospects, » *International Studies Quarterly*, vol 45 n°3, 2001, pp 389-408
- CONNOLLY William E., « The ‘New Materialism’ and the Fragility of Things. » *Millennium: Journal of International Studies*, vol. 41, no. 3, 2013, pp. 399–412.
- CONWAY Maura, « What Is Cyberterrorism? » *Current History*, vol. 101, n°659, Decembre 2002, pp. 436-442.
- COOLE Diana, « Agentic Capacities and Capacious Historical Materialism: Thinking with New Materialisms in the Political Sciences ». *Millennium*, vol. 41 n°3, 2013, pp. 451– 469
- CORRALES, Javier, et WESTHOFF Frank. « Information technology adoption and political regimes. » *International Studies Quarterly* vol. 50. n°4, 2006, pp. 911-933.
- COUPAYE Ludovic et DOUNY Laurence, « Dans la Trajectoire des Choses », *Techniques & Culture*, 52-53, 2009, pp. 12 – 39.
- COX Robert, « Social Forces, States, and World Orders », *Journal of International Studies*, 10 (2), juin 1981, p. 129.
- CROSS MAI'A DAVIS, « The Limits of Epistemic Communities: EU Security Agencies », *Politics and Governance*, vol 3, n°1, 2015 pp. 90-100.[1]

- CROSS MAI'A K. DAVIS. « Rethinking Epistemic Communities Twenty Years Later. », *Review of International Studies*, vol. 39 n°01, 2012, pp. 137–160.
- CUKIER, Kenneth Neil. « Who Will Control the Internet? Washington Battles the World. » *Foreign Affairs*, vol. 84, no. 6, 2005, p. 7- 13
- CURTIS Simon., & Koivisto, Marjo. « Towards a second “second debate”? Rethinking the relationship between science and history in international theory ». *International Relations*, 24, décembre 2010, pp. 433-455.
- DAGIRAL Éric. « Administration Électronique. » *Communications*, vol. 88, no. 1, 2011, pp. 9–17.
- DAGIRAL Éric. « Pirates, hackers, hacktivistes : déplacements et dilution de la frontière électronique », *Critique*, vol. 733-734, no. 6, 2008, pp. 480-495.
- DARTNELL Michael. « Weapons of Mass Instruction : Web Activism and the Transformation of Global Security. » *Millennium*, vol. 32, no. 3, Dec. 2003, pp. 477–499,
- DAUTANCOURT Vincent. « Les minorités russes en Estonie : unité et diversification », *Hérodote*, vol. 128, no. 1, 2008, pp. 73-85,
- DAVIES Owen, « Robotic Warriors Clash in Cyberwars, » *Omni*, vol. 9, n°4, janvier 1987.
- DE LANGHE Rogier, WEBER Erik, VAN BOUWE Jeroen, « A pragmatist approach to the plurality of explanations in International Relations Theory Graham Allison’s account of the Cuban Missile Crisis reconsidered » *6th Pan-European conference on international relations, Proceedings, The Standing Group of International Relations of the ECPR*, 2007, 17 p.
- DEDEHAYIR Ozgur et MÄKINEIF Saku J., « Dynamics Of Reverse Salience As Technological Performance Gap: An Empirical Study Of The Personal Computertechnology System. » *Journal of Technology Management & Innovation*, vol. 3, no. 3, 2008, pp. 55 – 66.
- DEIBERT Ronald J. et ROZOHINSKI Rafal : « Risking Security: Policies and Paradoxes of Cyberspace Security », *International Political Sociology* vol. 4, n° 1 pp. 15 - 32, 2010
- DEIBERT Ronald J., « Black Code: Censorship, Surveillance, and the Militarization of Cyberspace, » *Millennium*, vol. 32. n°33, décembre 2003, pp. 501-530

- DELMAS Richard, « L'Internet, gouvernance d'un monde incertain », *Revue française d'administration publique*, vol. 110, no. 2, 2004, pp. 217-224
- DENARDIS Laura, « Governance at the Internet's Core: The Geopolitics of Interconnection and Internet Exchange Points (IXPs) in Emerging Markets », *Conférence 2012 TRPC Research Conference on Communications, Information and Internet Policy, mars 2017.*
- DENNING Dorothy E., « Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy », *Global Problem Solving Information Technology and Tools*, Decembre 1999, 30 p.
- DER DERIAN James, « Cyber-deterrence » *Wired*, Vol. 2, n°. 9, septembre 1994.
- DER DERIAN James, « Foucault et les Autres : rencontres critiques dans le domaine des relations internationales », *Revue internationale des sciences sociales*, 2007/1 (n° 191), p. 77-82.
- DER DERIAN James. « The Question of Information Technology in International Relations. » *Millennium*, vol. 32, no. 3, décembre. 2003, pp. 441–456,
- DERIAN JAMES, "Cyberwar, Video Games, and the New World Order", *Second Annual Cyberspace Conference, Santa Cruz*, Avril 1991
- DERRIDA JACQUES, « Signature Events Context », *Glyph*, vol. 1 Baltimore, Johns Hopkins University Press, 1975 pp. 172 – 197.
- DEUDNEY Daniel et IKENBERRY Gilford John. « The Nature and Sources of Liberal International Order. », *Review of International Studies*, vol. 25, no. 2, 1999, pp. 179–196.
- DIAZ, Frédéric. « « coproduction » de la sécurité : une nouvelle forme de l'interventionnisme étatique pour une meilleure sécurité du public ? (le cas de grands rassemblements de populations en france) », *Déviance et Société*, vol. 27, no. 4, 2003, pp. 429-458.
- DION Stéphane. « Erhard Friedberg et l'analyse stratégique », *Revue française de science politique*, 43^e année, n°6, 1993. pp. 994-1008.
- DOGAN Mattei, « The Hybridization of Social Science Knowledge », *Library Trends*, vol. 45, n° 2, 1996, pp. 299-301.

- DOSI Giovanni « Technical paradigms and technical trajectories: the determinants and directions of technical change and the transformation of the economy », *Research Policy*, 11, 1982 pp. 147-162.
- DOSI Giovanni, « Sources, procedures and microeconomic effects of innovation », *Journal of Economic Literature*, 26, 1988, pp. 126-173.
- DOUZET Frédéric et DESFORGES Alix, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », *Netcom*, 32-1/2, 2018, pp. 87-108.
- DOYLE Michael W. « Kant, Liberal Legacies, and Foreign Affairs », *Philosophy and Public Affairs*, Vol. 12, No. 3, Eté, 1983, pp. 205-235.
- DRAKE William J., et Nicolaïdis Kalypso. « Ideas, Interests, and Institutionalization: ‘Trade in Services’ and the Uruguay Round. » *International Organization*, vol. 46, no. 1, 1992, pp. 37–100.
- DREZNER Daniel W., « The Global Governance of the Internet: Bringing the State Back In, » *Political Science Quarterly*, vol. 199 n°3, 2004, pp. 477-498.
- DRORI Gili S., et JANG YONG Suk « The global digital divide: A sociological assessment of trends and causes. » *Social Science Computer Review* vol. 21 n° 2, 2003, pp. 144-161.
- DUBOIS Michel, « From Discovery to Invention », *Revue européenne des sciences sociales*, 52-2, 2014, p. 7 – 42.
- DUCHASTEL Jean « Discours et informatique : des objets sociologiques ? », *Sociologie et sociétés* 252, 1993, pp. 157–170.
- DUPONT Benoît, « La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale », *Cultures & Conflits*, 2016/2 (n° 102), pp. 95 – 120.
- DURKHEIM Emile et MAUSS Marcel, « Note sur la notion de civilisation », *L'année sociologique*, n°12, 1913, pp. 46-50.
- DURKHEIM Emile, « Représentations individuelles et représentations collectives » *Revue de Métaphysique et de Morale*, tome VI, mai 1898.
- DUROSELLE Jean-Baptiste, « L'étude des relations internationales. Objet, méthodes, perspectives », *Politique étrangère*, décembre 1952, pp 229 - 232.
- EASTON David. « An approach to the analysis of political systems. », *World politics*, vol. 9.,n° 3, 1957, pp. 383-400.

- EDWARDS Paul Norris « Border Wars: The Science and Politics of Artificial Intelligence », *Radical America* vol. 19, no. 6, 1986, pp 39-50.
- ELINOR Ostrom et ELOI Laurent, « Par-delà les marchés et les États. La gouvernance polycentrique des systèmes économiques complexes », *Revue de l'Observatoire français des conjonctures économiques*, n° 120, 2012, pp. 13-72,
- ERIKSSON Johan, et GIAMPIERO Giacomello, « The Information Revolution, Security, and International Relations : (IR)Relevant Theory ? » *International Political Science Review*, vol. 27, no. 3, 2006, pp. 221–244.
- FARRELL Henry, « Constructing the International Foundations of E-Commerce : The EU-US Safe Harbor Agreement », *International Organization*, vol. 57 n°2, 2003, pp. 277-306.
- FAVRE Pierre, « La connaissance politique comme savoir légitime et comme savoir éclaté. », *Revue Française de Science Politique*, 1983, pp. 467-503.
- FEENBERG Andrew, « Marcuse or Habermas: Two critiques of technology », *Inquiry*, vol. 39, n°1, 1996, pp. 45-70.
- FIALAIRE Jacques. « L'évolution des politiques d'informatisation de l'administration publique en France. Quelles articulations entre services centraux et déconcentrés de l'État ? », *Politiques et management public*, vol. 10, n° 4, 1992. pp. 55-63.
- FINNEMORE Martha, et HOLLIS Duncan B « Constructing Norms for Global Cybersecurity. » *American Journal of International Law*, vol. 110, no. 3, 2016, pp. 425–479
- FINNEMORE Martha, KATHERYN Sikkink, « TAKING STOCK: The Constructivist Research Program in International Relations and Comparative Politics », *Annual Review of Political Science*, 4:1, 2001, pp. 391-416
- FINNEMORE Martha. et SIKKINK Katheryn « International norm dynamics and political change ». *International Organization* , vol. 52 n°4, pp. 887–917.
- FLICHY Patrice. « L'individualisme connecté entre la technique numérique et la société », *Réseaux*, vol. no 124, no. 2, 2004, pp. 17-51.
- FØRLAND Tor Egil, « The Ideal Explanatory Text in History: A Plea for Ecumenism », *History and Theory*, Volume 43, Issue 3, Oct. 2004, pp. 321–340

- FRASSON-QUENOZ Florent, « An inclusive map of international relations theories and authors », *Cahiers du CIPE* (Cuardernos del Centro de Investigaciones y Proyectos Especiales), Université Externado de Colombie, n°21, juin 2014, p. 21.
- FRIEDRICH S Jörg, « International Relations Theory in France ». *Journal of International Relations and Development*, janvier 2001, pp 118 - 137.
- FRUCHTERMAN Thomas .M.J. et REINGOLD, Edward. M. « Graph Drawing by Force-directed Placement », *Software - Practice and Experience*, 21, 1991.
- FUTTER Andrew, « ‘Cyber’ Semantics: Why We Should Retire the Latest Buzzword in Security Studies. » *Journal of Cyber Policy*, vol. 3, n°2, avril 2018, pp. 201–216.
- GALLIE Walter B. , « Essentially Contested Concepts », *Proceedings of the Aristotelian Society* vol. 56, 1955, pp .167 - 198.
- GARDEY Delphine, « Au cœur à corps avec le Manifeste Cyborg de Donna Haraway », *Esprit*, mars-avril 2009, pp. 208-217.
- GARNHAM Nicholas, GAMBERINI Marie-Christine (trad.), « La théorie de la société de l'information en tant qu'idéologie : une critique », *Réseaux*, volume 18, n°101, 2000 pp. 53-91
- GARTZKE Erik et Lindsay Jon R., « Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. », *Security Studies*, vol. 24, n°2, 2015, pp. 316-348.
- GARTZKE Erik, « The Myth of Cyberwar, Bringing War in Cyberspace Back Down to Earth », *International Security*, vol. 38, No. 2, 2013, pp. 41–73.
- GIBSON William, « Burning Chrome », *Omni*, N° 46, juillet 1982 pp 72 - 77.
- GEOGHEGAN, Bernard D. « The Historiographic Conceptualization of Information : A Critical Survey », *IEEE Annals of the History of Computer*, vol. 30 n°1, 2008, pp. 66-81.
- GOEMANS Hein E. et Schultz Kenneth A., « The Politics of Territorial Claims: A Geospatial Approach Applied to Africa, », *International Organization*, vol. 71, no. 1, janvier 2017, pp. 31–64.
- GOLDMAN Emily O. « Introduction: Information Resources and Military Performance. » *Journal of Strategic Studies*, vol. 27, no. 2, 2004, pp. 195–219.
- GOLLAC Michel, « Des chiffres insensés ? Pourquoi et comment on donne un sens aux données statistiques », *Revue française de sociologie*, n°38, 1997, p. 12

- GONZALEZ Antonio et Jouve Emmanuelle, « Minitel : histoire du réseau télématique français », *Flux*, vol. 47, no. 1, 2002, pp. 84-89.
- GOODMAN Will, « Cyber Deterrence Tougher in Theory than in Practice ? », *Strategic Studies Quarterly*, automne 2010, pp. 102-135.
- GOUGH Clair et Shackley Simon. « The respectable politics of climate change: The epistemic communities and NGOs », *International Affairs*, Vol. 77, No. 2, avril 2001, pp. 329-345
- GOUGH Clair, et Shackley Simon. « The Respectable Politics of Climate Change: The Epistemic Communities and NGOs », *International Affairs*, vol. 77, no. 2, 2001, pp. 329–345
- GRANJON Fabien, « La réduction de la fracture numérique », *Regards sur l'actualité*, n°327, La Documentation française, janvier 2007.
- GRINT Keith et Woolgar Steve. « On Some Failures of Nerve in Constructivist and Feminist Analyses of Technology. » *The Gender-Technology Relation*, 1995, pp. 48–75.
- GUARESI Magali, « Les thèmes dans le discours électoral de candidature à la députation sous la Cinquième République. Perspective de genre (1958-2007) », *Mots, Les langages du politique*, n°108, 2015, 180 p.
- GUCHET Xavier, « Pensée technique et philosophie transcendante », *Archives de Philosophie*, 1/2003 (Tome 66), p. 119-144.
- GUILLEN Mauro F., et SUAREZ Sandra L. « Explaining the global digital divide: Economic, political and sociological drivers of cross-national Internet use. » *Social forces*, vol. 84 n°2, 2005, pp. 681-708.
- GUITTON Clement. « Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK? », *European Security*, vol. 22, no. 1, 2013, pp. 21–35.
- HAAS Peter M. « Do regime matter? Epistemic community and Mediterranean Pollution Control », *International Organization*, vol. 43 (3), 1989, pp. 377 – 403.
- HAAS Peter M. « Introduction: Epistemic communities and international policy coordination », *International Organization*, vol. 46(1), 1992, pp. 1-35.
- HADDAD, Saïd. « Une grammaire de la cybersécurité française ou la construction d'une stratégie nationale de cyberdéfense (2008-2017) », *Stratégique*, vol. 117, no. 4, 2017, pp. 119-135.

- HAIN Jean-Yves, « Rationalités et relations internationales : l'inaccessible synthèse ? », *Cultures & Conflits*, 36, hiver 1999 - printemps 2000, pp. 5 -10.
- HALL Peter A. « Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain », *Comparative Politics*, vol. 25, no. 3, 1993, pp. 275–296.
- HAMELIN, Fabrice. « Le combattant et le technocrate. La formation des officiers à l'aune du modèle des élites civiles », *Revue française de science politique*, vol. 53, no. 3, 2003, pp. 435-463.
- HANNES Ebert et Maurer Tim, « Revendications sur le cyberspace et puissances émergentes », *Hérodote*, vol. 152-153, no. 1, 2014, pp. 276-295.
- HANSEN Lene et NISSENBAUM Helen, « Digital Disaster, Cyber Security, and the Copenhagen School », *International Studies Quarterly*, vol. 53, 2009, pp. 1155–1175.
- HANSEN Lene, et NISSENBAUM Helen. « Digital Disaster, Cyber Security, and the Copenhagen School. » *International Studies Quarterly*, vol. 53, no. 4, 2009, pp. 1155–1175.
- HARAWAY Donna, « A Cyborg Manifesto : Science, Technology, and Socialist-feminism in 80's », *Socialist Review* 15, no. 2, 1985.
- HARKNETT Richard J., CALLAGHAN John "P. et KAUFFMAN Rudi « Leaving Deterrance Behind : War-Fighting and National Cybersecurity. » *Journal of Homeland Security & Emergency Management*, Vol. 7, No 1, article 22, 2010.
- Harknett Richard, « Information Warfare and Deterrence », *Parameters : US Army War College Quartetly*, vol. 26, n°. 3, 1996, pp. 93-107
- HELLMANN Gunther (dir.), « The Forum : Are Dialogue and Synthesis Possible in International Relations ? », *International Studies Review*, vol. II, 2003.
- HELLMANN Gunther « Brother, Can You Spare a Paradigm? (Or Was Anybody Ever a Realist?) ». *International security*, 25(1), 2000 pp. 169 – 174
- HERMANN Margaret, « One Field, Many Perspectives: Building the Foundations for Dialogue: 1998 ISA Presidential Address », *International Studies Quarterly*, Volume 42, Issue 4, 1 Déc. 1998, pp. 605–624,
- HERRERA Geoffrey L. « Technology and International Systems. » *Millennium*, vol. 32, no. 3, décembre 2003, pp. 559–593.

- HERZ John H., « Idealist Internationalism and the Security Dilemma », *World Politics*, Vol. 2, N° 2, Janvier 1950, pp. 157–180
- HILLERY George A. Jr. « Definitions of Community : Areas of Agreement », *Rural Sociology*, vol. 20, n° 1, 1995, pp. 111-123
- HOTTOIS Gilbert, « Ethique et techno-science », *La pensée et les hommes*, n° 22, 1978 pp. 111 – 116.
- HOTTOIS Gilbert. « La technoscience : de l'origine du mot à ses usages actuels », *Recherche en soins infirmiers*, vol. 86, no. 3, 2006, pp. 24-32.
- HUYSMANS Jeff, « Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security », *Alternatives*, 27, supplément, 2002, pp 41 - 62.
- ISCHY Frédéric, « La « société de l'information » au péril de la réflexion sociologique ? », *Revue européenne des sciences sociales*, XL-123, 2002
- JACKSON Patrick Thaddeus et NEXON Daniel H., « Paradigmatic Faults in International-Relations Theory », *International Studies Quarterly*, vol. n° 53, n° 4, 2009, pp. 907 - 940.
- JACQUIER Claude, « Qu'est-ce qu'une communauté ? En quoi cette notion peut-elle être utile aujourd'hui ? », *Vie sociale*, 2011/2 (N° 2), p. 33-48.
- JORDAN Andrew et GREENAWAY John « Shifting Agendas, Changing Regulatory Structures And The ‘New’ Politics Of Environmental Pollution : British Coastal Water Policy, 1955–1995 ». *Public Administration*, 76, 1998, pp. 669-694.
- JUNIO Timothy J. « How Probable is Cyber War?: Bringing IR Theory Back In to the Cyber Conflict Debate, » *The Journal of Strategic Studies*, vol. 36, n°1, février 2013.
- KATZENSTEIN Peter J. et SIL Rudra « What is analytic eclecticism and why do we need it ? A pragmatist Perspective on Problems and Mechanisms in the Study of World Polities », intervention au colloque annuel de l'American Political Science Association le 1er septembre 2005.
- KEENAN Thomas, « Looking like Flames and Falling like Stars: Kosovo, “the First Internet War” », *Social Identities*, vol. 7, no. 4, 2001, pp. 539–550
- KEMPF Olivier, « Cyberstratégie à la française », *Revue internationale et stratégique*, 2012 n° 87, pp. 121-129. J
- KEOHANE Robert, « International institutions : two approaches », *International Studies Quarterly*, vol. 32, n°4, 1988, pp. 379-396.

- KEOHANE, Robert Owen et NYE Joseph S., « Power and Interdependence in the Information Age. » *Foreign Affairs*, vol. 77, no. 5, 1998, p. 81 – 94.
- KESA Katerina, « Estonie : une représentation du monde singulière, postsoviétique et européenne », *Anatoli*, n°2, 2011, pp. 63-77.
- KIM Chon-Kyun « A Cross-National Analysis of Global E-Government.», *Public Organization Review*, vol. 7 n°4, 2007, pp:317–329.
- KORANY Bahgat. « Un, deux, ou quatre... : Les écoles de relations internationales ». *Études internationales* 15, no 4, décembre 1984, pp. 699–723
- LACY Mark et PRINCE Daniel, « Securitization and the Global Politics of Cybersecurity. », *Global Discourse*, vol. 8, no. 1, 2018, pp. 100–115
- LAW John, « Objects and Spaces. », *Theory, Culture & Society*, vol. 19, n°. 5–6, 2002, pp. 91–105.
- LE BART Christian, « L'analyse du discours politique : de la théorie des champs à la sociologie de la grandeur », *Mots. Les langages du politique*, 72, 2003.
- LE FLOCH Guillaume. « Le sommet mondial de Tunis sur la société de l'information », *Annuaire français de droit international*, volume 51, 2005. pp. 464-486.
- LEE Edward, A., « Cyber-Physical Systems - Are Computing Foundations Adequate? », *Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, Austin, Texas, octobre 2006.
- LEGALLOIS Dominique, « La colligation : autre nom de la collocation grammaticale ou autre logique de la relation mutuelle entre syntaxe et sémantique ? », *Corpus*, n°11, 2012, pp. 31 -54.
- LICKLIDER Joseph Carl Robnett, « Man-Computer Symbiosis » *IRE Transactions on Human Factors in Electronics*, Mars 1960, p.4.
- LIEBERMAN Marvin B. et MONTGOMERY David B.. « First-Mover Advantages. » *Strategic Management Journal*, vol. 9, no. S1, 1988, pp. 41–58
- LIFF Adam P., « Cyberwar: A New “Absolute Weapon”? The Proliferation of Cyberwarfare Capabilities and Interstate War », *Journal of Strategic Studies*, vol. 35 n°3, juin 2012, pp. 401–428.
- LIFF Adam P., « The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio. » *Journal of Strategic Studies*, vol. 36, no. 1, 2013, pp. 134–138.

- LIJPHART Arend, « The Structure of the Theoretical Revolution in International Relations », *International Studies Quarterly*, Vol. 18, No. 1, Mars 1974, pp. 41-74.
- LINDEMANN Thomas « Les guerres américaines dans l'après-guerre froide : entre intérêt national et affirmation identitaire ». *Raisons politiques*, 13 (1), 2004, pp . 37-57.
- LINKLATER Andrew, « The ‘Standard of Civilisation’ in World Politics », *Social Character, Historical Processes*, vol. 5, 2, juillet 2016.
- LIPSCHUTZ Ronnie D. « Reconstructing World Politics – the Emergence of Global Civil Society, » *Millennium* vol. 21, n°3, 1992, pp. 389-420.
- LOHARD Audrey, « La genèse inattendue du cyberspace de William Gibson », *Quaderni : Cyberesp@ce & territoires*, Vol. 66, N°1, 2008 pp. 11-13.
- LONSDALE David J. « Information Power: Strategy, Geopolitics, and the Fifth Dimension. » *Journal of Strategic Studies*, vol. 22, no. 2-3, 1999, pp. 137–157.
- LOVELUCK Benjamin. « Internet, une société contre l’État ? Libéralisme informationnel et économies politiques de l’auto-organisation en régime numérique », *Réseaux*, vol. 192, no. 4, 2015, pp. 235-270.
- MACKAY, Hughie, and GILLESPIE Gareth. « Extending the Social Shaping of Technology Approach: Ideology and Appropriation. » *Social Studies of Science*, vol. 22, no. 4, Nov. 1992, pp. 685–716,
- MACKENZIE Donald « Marx and the Machine », *Technology and Culture*, Vol. 25, No. 3. juillet, 1984, pp. 473-502.
- MACLEOD Alex, « Les études de sécurité : du constructivisme dominant au constructivisme critique », *Cultures & Conflits*, 54, 2004, pp.13-51.
- MAINGUENEAU Dominique, « Analyse du discours et archive », *Semen*, 8, 1993.
- MANJIKIAN Mary. « From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. » *International Studies Quarterly*, vol. 54, no. 2, 2010, pp. 381–401.
- MANSFIELD, Edward D. et PEVEHOUSE Jon. « Democratization and the Varieties of international Organizations. », *Journal of Conflict Resolution*, 52(2), 2008, pp. 269-294.
- MARTIN Clément et PAJON Christophe, « La sociologie militaire par les personnels de la défense : une sociologie d’insiders ? », *Les Champs de Mars*, 2015/2 (N° 27), pp. 23-30.
- MARTINEZ William, « Au-delà de la cooccurrence binaire... Poly-cooccurrences et trames de cooccurrence », *Corpus*, n°11, 2012, pp. 191 – 218.

- MARTRES Jean-Louis, « De la nécessité d'une théorie des relations internationales : l'illusion paradigmique », *Annuaire Français de Relations Internationales*, vol. IV, 2003, pp. 22-28.
- MARTRES Jean-Louis, « De la nécessité d'une théorie des relations internationales : l'illusion paradigmique », *AFRI*, Vol. IV, 2003, pp. 19 - 41.
- MASSIT-FOLLEA Françoise, « Internet et les errances du multistakeholderism », *Politique étrangère*, 2014/4 (Hiver), p. 29-41.
- MASSIT-FOLLEA Françoise, « De la régulation à la gouvernance de l'internet. Quel rôle pour les usagers-citoyens ? », *Les Cahiers du numérique*, vol. 3, no. 2, 2002, pp. 239-263.
- MASTERTON, Rear et al. « New Concepts in Global War-gaming », *Proceedings—US Naval Institute*, juillet 1987, pp. 117-119.
- MATTELART Armand, « L'âge de l'information : genèse d'une appellation non contrôlée ». *Réseaux*, 101, 2000, pp 21-52
- MAUSS Marcel, « The Problem of Nationality », *Proceedings of the Aristotelien Society, Londres*, 1920, pp. 242 - 251.
- MAUSS Marcel, « Essai sur le don. Forme et raison de l'échange dans les sociétés archaïques », *l'année sociologique*, seconde série, 1923-1924, tome 1.
- MAUSS Marcel, « la nation », *l'année sociologique*, 3ème série, 1953, pp. 7-68.
- MAUSS Marcel, « les techniques du corps », *Journal de psychologie normale et pathologique*, n°32, 1935, pp. 271-293.
- MAYAFFRE Damon, « De l'occurrence à l'isotopie. Les co-occurrences en lexicométrie », *Sémantique & Syntaxe*, n°9 p. 53 à 72, 2008.
- Mayaffre Damon et Viprey Jean-Marie (dir.) « la cooccurrence : du fait statistique au fait textuel », *Corpus*, n°11, 2012.
- MAYAFFRE Damon, « Introduction » In. « Les corpus politiques : objet, méthode et contenu », *Corpus*, 4, 2005.
- McCULLOCH Warren, et Pitts Walter, « A logical calculus of the ideas immanent in nervous activity », *Bulletin of Mathematical Biophysics*, University of Chicago Press, 1943.

- MERAND Frédéric et POUILOT Vincent, « Le monde de Pierre Bourdieu : Éléments pour une théorie sociale des Relations internationales », *Revue canadienne de science politique*, vol. 41 n°3, 2008, pp. 603 – 625.
- MEYER Morgan, et Molyneux-Hodgson Susan « « Communautés épistémiques » : une notion utile pour théoriser les collectifs en sciences ? », *Terrains & travaux*, vol. 18, no. 1, 2011, pp. 141-154.
- MICHAUD Thomas, « La dimension imaginaire de l’innovation : l’influence de la science-fiction sur la construction du cyberespace », *Innovations*, n° 44, 2014/2, pp 213 - 233.
- MILLIKEN Jennifer. « The Study of Discourse in International Relations : A Critique of Research and Methods. » *European Journal of International Relations*, vol. 5, no. 2, Juin 1999, pp. 225–254,
- MITRA Raja. « Emerging state-level ICT development strategies » Information and communication technology in development: Cases from India, 2000, pp.195-205.
- MOL Annemarie et LAW John, « Regions, networks and fluids: anaemia and social topology. » *Social studies of science*, vol. 24, n°4, 1994, pp. 641-671.
- MONJARDET Dominique, « Le chercheur et le policier. L’expérience des recherches commanditées par le ministère de l’Intérieur », *Revue française de Science politique* n°2, 47e année, 1997, pp. 211-225.
- MÜLLER Birgit, « Comment rendre le monde gouvernable sans le gouverner : les organisations internationales analysées par les anthropologues », *Critique internationale*, 54, pp. 9-18.
- MURPHY Emma C. « Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere. » *International Studies Quarterly*, vol. 53, no. 4, 2009, pp. 1131–1153
- MUSSO Pierre, « Le cyberespace, figure de l’utopie technologique réticulaire », *Sociologie et sociétés*, Vol. 32, n° 2, automne 2000, pp. 31 – 56.
- MUSSO Pierre, « Le Web : nouveau territoire et vieux concepts », *Annales des Mines - Réalités industrielles*, 2010/4, Novembre 2010, pp. 75-83.
- NEWMAN Abraham L. « Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive. », *International Organization*, vol. 62, no. 01, 2008, pp. 103 – 130.
- NEWMYER Jacqueline, « The Revolution in Military Affairs with Chinese Characteristics, » *Journal of Strategic Studies*, vol. 33 n°4, 2010, pp. 483-504.

- NISSENBAUM Helen « Where Computer Security Meets National Security ». *Ethics and Information Technology*, vol. 7, n° 2, 2005, pp. 61–73.
- NYE Joseph S., « Nuclear lessons for cyber security? », *Stratetegic Studies Quarterly*, vol. 5 n°4, 2011, pp. 18–38.
- NYE Joseph S., « The Changing Nature of World Power », *Political Science Quarterly*, vol. 105, n ° 2, été 1990, pp. 177-192.
- OGER Claire et OLLIVIER-YANIV Caroline, « Analyse du discours institutionnel et sociologie compréhensive : vers une anthropologie des discours institutionnels », *Mots. Les langages du politique*, 71, 2003
- PAGANINI Pierluigi, « Zero-Day Exploits in the Dark », *Infosec Institute*, 21 avril 2015. <http://resources.infosecinstitute.com/zero-day-exploits-in-the-dark/> [consulté le 1er août 2016].
- PERRIN Jean-François, « Jean Carbonnier et la sociologie législative », *l'année sociologique*, Vol. 57, 2007, pp. 403-415.
- PETERSON John « Decision-making in the European Union : towards a framework of analysis », *Journal of European Public Policy*, vol. 2, n°1, 1995, pp. 69 – 93.
- PETITEVILLE Franck, « Les organisations internationales dépolitisent-elles les relations internationales ? », *Gouvernement et action publique*, 2016/3, pp. 113-129.
- PIERCE Charles S. « On the Natural Classification of Arguments », *Proceedings of the American Academy of Arts and Sciences*, vol. 7, 1867, pp. 261–287.
- PIERSON Paul, « Increasing Returns, Path Dependence, and the Study of Politics », *American Political Science Review*, n°94 (2), 2000, pp. 251 – 267.
- PIERSON Paul. « Increasing returns, path dependence, and the study of politics. », *American political science review* vol. 94 n° 2, 2000, pp. 251-267.
- PINCH, Trevor J. et BIJKER Wiebe E. , « The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. », *Social Studies of Science*, vol. 14, n°. 3, 1984, pp. 399–441.
- PORTE Rémy, « Officier d'active et historien est-il indispensable d'être schizophrène ? », *Les Champs de Mars*, 2015/2 (N° 27), p. 59-66.
- PROULX Serge. « La Sociologie Des Usages, Et Après ? » *Revue Française Des Sciences De l'Information Et De La Communication*, n°6, Janvier 2015.

- QUERE Louis., « La situation toujours négligée ? », *Réseaux*, volume 15, n°85, 1997, pp. 163-192.
- RADAELLI Claudio M. « Logiques de pouvoir et récits dans les politiques publiques de l'Union européenne », *Revue française de science politique*, n°2, 2000. pp. 255-275
- RADAELLI, Claudio M., « Harmful Tax Competition in the EU: Policy Narratives and Advocacy Coalition », *Journal of Common Market Studies*, 37, 1999, pp 661-682.
- RAILTON, Peter, « Probability, explanation, and information ». *Synthese* 48, 1981, pp. 233 - 256.
- RAMEL Frédéric, « Marcel Mauss et l'étude des relations internationales : un héritage oublié », *Sociologie et sociétés*, vol. 36, n° 2, 2004, pp. 227-245.
- RAUS Rachèle, « Productivité de cyber et hyper dans le lexique français d'Internet », *La linguistique* 2/2001, Vol. 37, pp. 71-88
- REARDON Robert et CHOUCRI Nazli, « The Role of Cyberspace in International Relations: A View of the Literature », 53ème Convention annuelle de l'ISA « Power, Principles, and Participation in the Global Information Age », San Diego, États-Unis, 1er au 4 avril 2012.
- REINERT Max, « Alceste, une méthodologie d'analyse des données textuelles et une application : Aurélia, de Gérard de Nerval », *Bulletin de méthodologie sociologique*, vol. 26, n°1, 1990, pp. 24–54.
- RID Thomas et MCBURNEY Peter, « Cyberweapons », *The RUSI Journal*, Volume 157, Issue 1, 2012.
- RID Thomas, « Cyber War Will Not Take Place », *Journal of Strategic Studies*, vol. 35, n°1, octobre 2011.
- RISSE Thomas, « Let's Argue!': Communicative Action in World Politics. » *International Organisazation*, vol. 54, n°1 2000, pp 1-41.
- RODRIGO, Pierre. « Marx et la technique », *Philosophie*, vol. 133, no. 2, 2017, pp. 37-51.
- ROSENAU Pauline, « Once Again into the Fray : International Relations Confronts the Humanities », *Millennium*, 19 (1), 1990, p. 48
- ROSENBLUETH Arturo, WIENER Norbert et BIGELOW Julian, « Behavior, Purpose and Teleology »,. *Philosophy of Science*, 10:, 1958, pp. 18-24
- ROSENBLUETH Arturo, WIENER Norbert et BIGELOW Julian, « Comportement, intention et télologie », *Les Etudes Philosophiques*, 2, 1961, pp. 147-56.

- RUGGIE John Gerard, « What Makes the World Hang Together? Neo-utilitarianism and the Social Constructivist Challenge », *International Organization*, vol. 52, n°4, 1998, pp. 855-885.
- RUTHS Derek et PFEFFER Jürgen, « Social media for large studies of behavior. », *Science*, vol. 346, n° 6213, 2014, pp. 1063-1064.
- SANDAL Nuhket A., « Religious Actors as Epistemic communities in Conflict Transformation: the cases of South Africa and Northern Ireland », *Review of International Studies*, n° 27 (3), 2011, pp. 929 – 949.
- SANDAL Nukhet.. « Religious actors as epistemic communities in conflict transformation: The cases of South Africa and Northern Ireland. » *Review of International Studies*, Vol. 37, 2011, pp. 929 – 949.
- SANDHOLTZ Wayne, « Dynamics of International Norm Change: Rules against Wartime Plunder » *European Journal of International Relations*, Vol 14, Issue 1, mars 2008, pp. 101 – 131.
- SHAH Dhavan V., CAPPELLA Joseph N., et NEUMAN W. Russell « Big data, digital media, and computational social science: Possibilities and perils. », *The ANNALS of the American Academy of Political and Social Science*, vol. 659 n°1, 2015, pp. 6-13.
- SCHUURMAN Frans J. « Paradigms Lost, Paradigms Regained? Development Studies in the Twenty-First Century. » *Third World Quarterly*, vol. 21, no. 1, 2000, pp. 7–20.
- SFEZ Lucien, « La technique comme fiction », *Revue européenne des sciences sociales*, XL-123, 2002, pp. 65 -74.
- SHACKELFORD Scott J., « Toward Cyberpeace: Managing Cyber attacks through Polycentric Governance », *American University Law Review*, vol 62, n°5, 2013, pp. 1273 – 1364
- SHACKELFORD Scott J., « Governing the Global Commons in International Law and Relations » Université de Cambrigde, 15 Nov, 2011. (non publié)
- SIMONNEAU Damien, « Regard critique sur le label ‘études critiques de sécurité’ », *Études critiques de sécurité*. Vol. 46, N° 2-3, juin–septembre 2015.
- SKINNER Quentin, « Motives, Intentions and the Interpretation of Texts », *New Literary History*, vol. 3, n°2, 1972, p. 393-408.
- SMITH Steve, « Dialogue and the Reinforcement of Orthodoxy in International Relations », *International Studies Review*, Vol. 5, I1, Mars 2003, pp. 141–143,

- SOUTOU Georges-Henri. « La stratégie du renseignement : essai de typologie », *Stratégique*, vol. 105, no. 1, 2014, pp. 23-42.
- STONE John, « Cyber War Will Take Place! » *Journal of Strategic Studies*, vol. 36, no. 1, 2013, pp. 101–108.
- TABER Charles S. et TIMPONE Richard J.. « Beyond Simplicity: Focused Realism and Computational Modeling in International Relations. » *Mershon International Studies Review*, vol. 40, no. 1, 1996, pp. 41–79.
- TAGUIEFF Pierre-Alexandre, « L'idée de progrès une approche historique et philosophique » suivi de « Eléments de Bibliographie », », *Les Cahiers du CEVIPOF*, septembre 2002 / 32, 137 p.
- TANCZER Leonie Maria, BRASS Irina et CARR Madeline, « CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy », *Global Policy*, vol. 9, 2018, pp. 60–66.
- TEMPLE Dennis The Contrast Theory of Why-Questions », *Philosophy of Science*, 55, n° 1, mars 1988, pp. 141-151.
- ÜNVER Akin H., « Computational International Relations : What Can Programming, Coding and Internet Research Do for the Discipline ? », *All Azimuth: A Journal of Foreign Policy and Peace*, vol. 8, n°2, 2019, pp. 157-182.
- VALERIANO Brandon, et MANESS Ryan C. « The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11. » *Journal of Peace Research*, vol. 51, no. 3, 2014, pp. 347–360.
- VERNADSKY Vladimir I. , « The Biosphere and the Noosphere », *American Scientist*, (janvier) 1945, 33(1), p. 1-12.
- VERNANT Jacques, « Vers une sociologie des relations internationales », *Politique étrangère*, 1962, pp. 229-232.
- VINGE Vernor, « The coming Technological Singularity », in Vision-21: Interdisciplinary Science and Engineering in the Era of Cyberspace, *NASA Publication*, 1993, pp. 11–22
- VOS POST Jonathan, « Cybernecitic War », *Omni*, mai 1979, pp 44-50.
- WALSER Randal, « Autodesk Cyberspace Project », *Mondo 2000*, 02, 1992, p. 264.
- WALT Stephen M. « The Renaissance of Security studies », *International Studies Quarterly*, 35 (2), 1991, pp. 211-239.

- WALTZ Kenneth, « The Spread of Nuclear Weapons: More May Better », *Adelphi Papers*, N° 171, 1981,
- WEBER Claude, Perrottet Jean-Philippe, « La place de l'homme dans les enjeux de cybersécurité », *Stratégique*, 2017/4 (N° 117), pp. 83-98.
- WEINBLUM Sharon et Danero Iglesias, Julien, « The discursive exclusion of minorities: A study of identity discourse in Israel and Moldova », *Critical Approaches to Discourse Analysis across Disciplines Journal*, vol. 7 n°1, 2013, pp. 164-179
- WELDES Jutta, « Constructing National Interests », *European Journal of International Relations*, 2 (3), 1996, pp. 280 - 289.
- WINNER Langdon « Do Artifacts Have Politics? », *Daedalus*, Vol. 109, No. 1, Hiver 1980, pp. 121 - 136.
- WOOLGAR Steve et LEZAUN Javier, « The Wrong Bin Bag: A Turn to Ontology in Science and Technology Studies? », *Social Studies of Science*, vol. 43, no. 3, juin 2013, pp. 321–340,
- ZEHFUSS, Maja « Contemporary western war and the idea of humanity » In *Environment & Planning D: Society & Space*. 30, 5, 2012, pp. 861-876.
- ZIMMERN Alfred, «The Prospects for Democracy ». *International Affairs* 7, 3, 1928, pp. 153–191.[1]
- ZITO Anthony R. « Epistemic communities, collective entrepreneurship and European integration », *Journal of European Public Policy*, vol 8, n°4, 2001, pp. 585-603

Etudes

- ARQUILLA John et RONFELDT David, « The Emergence of Noopolitik: Toward An American Information Strategy », RAND Corporation, Santa Monica, 1999, 89 p.
- BAUDOT Pierre-Yves, La compatibilité des systèmes. L'informatique dans le jeu administratif : Préfectures, Collectivités Locales et ministère de l'Intérieur, 1966-1975, Rapport de post-doctorat, UMR CNRS 5206 Triangle, juin 2007, 95 p.
- BERNES-LEE, Tim, Information Management: A Proposal, CERN, mars 1989.
- DE FALCO Marco, Stuxnet Facts Report - A Technical and Strategic Analysis, NATO CCD COE Publications, 2012.

- DENECE Éric et ARBOIT Gérard, « Les études sur le renseignement en France », Rapport de Recherche n° 8, Centre Français de Recherche sur le Renseignement, Novembre 2009, p. 21
- DUBO Orlane, « Analyse comparée de la recherche en matière de cyberdéfense militaire », Rapport du Centre de recherche de l'armée de l'air, 2015, 51 p.
- EDWARDS Paul Norris, Artificial intelligence and high technology war: the perspective of the formal machine Silicon Valley Research Group, University of California, Santa Cruz, 1986, 90 p.
- JEANGENE-VILMER Jean-Baptiste, ESCORIA Alexandre, GUILLAUME Marine et HERRERA Janaina. Les Manipulations de l'Information, un défi pour nos démocraties, rapport conjoint du Centre d'analyse, de prévision et de stratégie (CAPS, ministère de l'Europe et des Affaires étrangères) et de l'Institut de recherche stratégique de l'École militaire (IRSEM, ministère des Armées), Paris, aout 2018, 214 p.
- KEDZIE Christopher R., Communication and Democracy: Coincident Revolutions and the Emergent Dictators. Santa Monica, RAND Corporation, 1997, 120 p.
- LIBICKI Martin C., Cyberdeterrence and Cyberwar,.Santa Monica, CA: RAND Corporation, 2009, 144 p.
- NYE Joseph S., Cyber power, Harvard Kennedy School, Belfer Center for Science and International Affairs, mai 2010, 30 p.

Vidéos et documentaires

- NEALE Mark, *No Maps For These Territories*, (4 novembre 2000), DVD, New Video Group, 25 novembre 2003.
- FLORIDI Luciano, « Where are we in the philosophy of information ? », University of Bergen, Norway. 21 juin 2016.

Index des noms d'auteurs

- ABELLA Alex, 308
ACUTO Michele, 42
ADLER Emanuel., 277
ADORNO Theodor, 445
AGRE Jonathan, 363
AKRICH Madeleine, 101, 150, 152, 153, 155, 273, 444, 453
ALAM Thomas, 109
ALBERTS David S, 363
ALDEN Chris, 414
ALDER Emanuel, 101
ALLISON Graham, 361
AMPERE André-Marie, 136
ANAND Menon, 277
ANDREWSKY Evelyne, 138
APTER Emily, 455
ARBOIT Gérard, 361
ARCHIBUGI Danielle, 409
ARON Raymond, 172
ARQUILLA John, 146, 308, 309, 381, 382, 423
ARSENE Séverine, 19
ASHBY William Ross, 163
ASHLEY Richard K., 56
ASIMOV Isaac, 139
AUFFRET Yves, 119, 191
AXELOS Kostas, 153
AYRES Robert, 165
AZUMA Ronald, 132
BACHELARD Gaston, 435
BACON Francis, 166
BAILLAT Alice, 53, 86, 87
BAIRD Zoë, 407
BAKIS Henry, 175
BALTES Paul, 270
BALZACQ Thierry, 27, 39, 58, 60, 65, 66, 67, 72, 82, 273, 289, 370, 473, 474, 475
BARBAROUX Pierre, 134, 301, 363
BARDINI Thierry, 182
BARNES Harry Elmer, 379
BARRY Andrew, 455
BARTHES Roland, 51, 55
BASLE Maurice, 154
BATTISTELLA Dario, 27, 28, 30, 35, 41, 42
BAUD Michel, 190, 308
BAUDOT Pierre-Yves, 173, 313, 314, 315, 383
BEARD Charles, 54
BEAU Francis, 361, 362
BELLAIS Renaud, 315
BENEDIKT Michael, 141, 465
BENIGER James R, 167
BERGER Peter, 26
BERNES-LEE Tim, 144
BERSINI Hugues, 143
BETZ David, 141
BIGELOW Julian, 137
BIGO Didier, 28, 56, 69, 70, 376
BIJKER Wiebe, 154, 155, 447, 448
BOCKEL Jean-Marie, 259
BOËNE Bernard, 111
BOMBERG Elizabeth, 277
BONDITTI Phillippe, 56
BOOTH Ken, 62
BOSSY Thibault, 280
BOURBEAU Philippe, 68
BOURDIEU Pierre, 50, 81, 82, 83, 172
BOUSSAGUET Laurie, 102, 279, 280
BOUTHERIN Grégory, 284
BRAUN Benjamin, 457
BRETON Philippe, 168
BROWN Chris, 409, 429
BRUCHILL Scott, 31
BRUCK Henry, 37
BRUNETEAU Bernard., 170
BRYANT William, 424
BULL Hedley, 62
BUTTERFIELD Herbert, 32
BUZAN Barry, 67, 73, 366, 369, 373, 394, 448
CALLON Michel, 155, 453, 454, 455, 515
CANT Sue, 188
ČAPEK Karel, 129
CARLSNAES Walter, 42
CARR Edward, 392
CARR Jeffrey, 188, 423
CASTELLS Manuel, 144, 168, 169, 176, 184, 410
CATTARUZZA Amaël, 297
CAVELTY Myriam Dunn, 365, 391, 421

- CAYROL Nicolas, 24
 CERF Vinton, 143
 CHAMBOREDON Jean-Claude,, 83
 CHAMPONNOIS Suzanne, 15
 CHARAUDEAU Patrick, 50, 88, 90
 CHARILLON Frédéric, 273
 CHATEAURAYNAUD Francis, 182
 CHAUMONT Jean-Michel, 353
 CHAZAL Gérard, 149, 163
 CHILSTEIN David, 322
 CHINN Menzie, 414
 CHOUCRI Nazli, 390, 424, 465, 467, 468,
 469, 471, 472
 CHOUCRI Nazli,, 465
 CICOUREL Aaron, 454, 515
 CLARK Ian, 343
 CLARKE Richard, 424
 CLEMENS Martin, 190
 CLYNES Manfred, 139
 COCKBURN Cynthia, 153
 COHENDET Patrick, 101
 COMAN Ramona, 25
 COMOR Edward, 410
 CONNOLLY William, 452
 CONWAY Maura, 373
 COOK Gary, 190
 COOLE Diana, 451, 453
 CORNUT Jérémie, 42, 43, 44, 45, 46, 47, 48,
 75, 88, 107, 436
 CORRALES, Javier, 416, 417
 COULOUBARITSIS Lambros, 148
 COUPAYE Ludovic, 154
 COX Robert, 54, 63
 CREPLET Frédéric, 101
 CRESPY Amandine, 25
 CROSS Mai'a, 101, 102, 270, 272, 275, 276,
 278
 CROZIER Michel, 292, 299, 357
 CUDWORTH Erika, 453
 CUKIER, Kenneth, 407
 CURTIS Simon, 37, 42
 CUSSET François, 378
 DAGIRAL Éric, 182, 314
 DANERO IGLESIAS, Julien, 86
 DANET Didier, 297
 DARTNELL Michael, 386, 388
 DAUTANCOURT Vincent, 15
 DAVID Paul, 155
 DAVIES Owen, 140, 381
 DE FALCO Marco, 191, 474
 DE LANGHE Rogier, 46
 DEDEHAYIR Ozgur, 450
 DEIBERT Ronald, 366, 367, 411, 412
 DELMAS Richard, 301
 DELORME Robert, 138
 DEMCHAK Chris C, 188
 DENARDIS Laura, 265
 DENAT Céline, 148
 DENECE Éric, 361
 DENNING Dorothy, 374
 DER DERIAN James, 38, 56, 381, 382, 384,
 429
 DERTOZOZOS, M.L, 167
 DESCHAUX-DUTARD Delphine, 415
 DESFORGES Alix, 135, 176
 DEUDNEY Daniel, 392
 DEVETAK Richard, 31
 DION Stéphane, 292
 DOBRY Michel, 57
 DODGE Martin, 175, 184
 DOGAN Mattei, 40
 DOLPHIJN Rick, 451
 DONOVAN James, 379
 DOSI Giovanni, 154
 DOUNY Laurence, 154
 DOUZET Frédéric, 176
 DOYLE Michael W., 32
 DRAKE William, 103, 277, 278, 282
 DREZNER Daniel, 394, 403
 DRORI Gili, 414
 DRUCKER Peter, 167
 DUBO Orlane, 330
 DUBOIS Michel, 153
 DUCHASTEL Jean, 52, 87
 DUNN CALVETY Myriam, 473, 474, 475
 DUNNE Timothy, 47
 DUPONT Benoît, 253, 263, 408
 DUPOUËT Olivier, 101
 DURKHEIM Emile, 97, 156, 174, 253, 444
 DUROSELLE Jean-Baptiste, 27
 DUVALL Raymond, 366
 ECKERSLEY Robyn, 429
 EDWARDS Paul Norris, 381
 EGLOFF Florian, 391
 ELIAS Norbert, 60, 160
 ELLUL Jacques, 151
 EMPRIN Fabien, 53, 86, 87
 ERIKSSON Johan, 390, 423

- ESCORIA Alexandre, 375
 EVRARD Aurélien, 280
 FAINZANG Sylvie, 353
 FAIRLIE Robert, 414
 FALQUE-PIERROTIN Isabelle, 319
 FARRELL Henry, 406, 407
 FAVRE Pierre, 25, 27
 FERRARY Michel, 454
 FIALAIRE Jacques, 314, 354
 FINNEMORE Martha, 73, 304
 FLAHERTY Bernard, 139
 FLICHY Patrice, 174
 FLORIDI Luciano, 145, 164
 FØRLAND Tor Egil, 45
 FOUCAULT Michel, 52, 56, 99
 FRASSON-QUENOZ Florent, 34
 FRIEDBERG Erhard, 292, 357
 FRIEDRICHS Jörg, 27
 FRUCHTERMAN Thomas, 209
 FUTTER Andrew, 438, 440
 GALLIE Walter, 58, 439
 GALLOUEDEC-GENUYS Françoise, 315
 GAMBERINI Marie-Christine, 169
 GARDEY Delphine, 139
 GARNHAM Nicholas, 169
 GARNOT Benoît, 353
 GASTON-GRANGER Gilles, 174
 GAUTRAUD Nathalie, 319
 GEOGHEGAN, Bernard, 162, 314
 GEORGE Éric, 168
 GHAMARI-TABRIZI Sharon, 308
 GIAMPIERO Giacomello, 390, 423
 GIBSON James William, 381
 GIBSON William, 124, 131
 GILLE Bertrand, 151
 GILLESPIE Gareth, 417
 GODIN Benoît, 164
 GOLLAC Michel, 197
 GONZALEZ Antonio, 317
 GOODMAN Will, 429
 GOUGH Clair, 104, 268
 GRANJON Fabien, 168, 173
 GRAY Chris Hables, 378, 379, 381
 GREENAWAY John, 280
 GRESLE François, 110
 GRINT Keith, 451
 GROS Frédéric, 56
 GROSS Michael Joseph, 189
 GRUA François, 24
 GUARESI Magali, 87, 201
 GUCHET Xavier, 150, 162
 GUILLAUME Marine, 375
 GUILLEN Mauro, 414
 GUISNEL Jean, 317
 GUITTON Clement, 420
 GURRUCHAGA Marion, 109
 GUSTERSON Hugh, 366
 HAAS Peter, 100, 101, 270, 276
 HABERMAS Jürgen, 40, 64, 149, 151
 HACHMEITER Lutz, 136
 HAINÉ Jean-Yves, 361
 HALL Peter, 276
 HALLIDAY Fred, 29
 HÅLLSTEN Henrik, 48
 HANNES Ebert, 415
 HANSEN Lene, 74, 365, 371, 433
 HARAWAY Donna, 139, 378, 382
 HARKNETT Richard, 188, 429
 HARREL Yannick, 146
 HAUBEN Micheal, 144
 HAUBEN Ronda, 144
 HAUTE (VAN) Emilie, 25
 HEIDEGGER Martin, 149
 HELD David, 63, 102
 HELLMANN Gunther, 41
 HERMANN Margaret, 45
 HERRERA Geoffrey, 397, 448
 HERRERA Janaina, 375
 HERZ, John H, 36, 393
 HINDUJA Sameer, 473
 HOBDEN Stephen, 453
 HOLLIS Duncan, 304
 HOLLIS Martin, 32
 HOLMES David, 386
 HOLZNER Burkart, 100
 HORKHEIMER Max, 61, 445
 HOTTOIS Gilbert, 378
 HUGHES Thomas, 155, 448, 449
 HUIITEMA Christian, 318
 HUSSEIN Kassim, 277
 HUYGHE François-Bernard, 188
 IKENBERRY Gilford John, 392
 ISCHY Frédéric, 166
 JACKSON Patrick Thaddeus, 30
 JACQUIER Claude, 97
 JAMESON Fredric, 381
 JANG Yong Suk, 414
 JEANGENE-VILMER Jean-Baptiste, 375

- JOHNSON Deborah, 317
 JONES Charles, 394, 448
 JORDAN Andrew, 280
 JORDAN Tim, 418
 JOUVE Emmanuelle, 317
 JUNIO Timothy, 425
 KAHN Robert, 143
 KALDOR Mary, 381
 KALINOWSKI Isabelle, 108
 KALYVAS Andréas, 73
 KAPLAN Fred, 308
 KATZENSTEIN Peter, 34, 41, 43, 73
 Kazancigil Ali, 14
 KECK Margaret, 38
 KEDZIE Christopher, 416
 KELSTRUP Morten, 70
 KEMPF Olivier, 188
 KEOHANE Robert, 34, 37, 41, 393, 396
 KESA Katerina, 14
 KIM Chon-Kyun, 414
 KING Gary, 37
 KLARE Michael, 380
 KLINE Nathan, 139
 KNAKE Robert, 424
 KNORR-CETINA Karin, 454, 515
 KOIVISTO, Marjo, 37
 KORANY Bahgat, 29
 KOWERT Paul, 73
 KRAMER Franklin, 418
 KRASNER Stephen D, 34, 41
 KREBS, Ronald R, 277
 KRIEG-PLANQUE Alice, 373
 KUEHL Daniel, 418
 KUEHL Daniel, 418
 KURKI Milja, 47, 394
 LA BRANCHE Stéphane, 56
 LABORDES Pierre, 259
 LABRIOLLE François, 15
 LACY Mark, 372
 LADMIRAL Jean-René, 149
 LAFFEY Mark, 366
 LAFFITE Jacques, 151
 LAFONTAINE Cécile, 138
 LASBORDES Pierre, 322, 324
 LASSWELL Harold, 465
 LATOUR Bruno, 100, 150, 155, 378, 453,
 454, 515
 LAUREL Brenda, 184
 LAVOREL Sabine, 415
 LAW John, 475
 LE BART Christian, 51
 LE GLOANNEC Anne-Marie, 69
 LEBRETON David, 184
 LEDEVEDEC Nicolas, 139
 LEE Edward, 297
 LEGALLOIS Dominique, 89
 LEGRO Jeffrey, 73
 LEMONNIER Pierre, 100, 150
 LEROI-GOURHAN André, 153
 LESSIG Lawrence, 407
 LEVY Jacques, 172
 LEZAUN Javier, 451
 LIBICKI Martin, 309
 LICKLIDER Joseph Carl Robnett, 139
 LIEBERMAN Marvin, 450
 LIFF Adam, 425, 426
 LIJPHART Arend, 37
 LINDSAY Jon, 426, 428
 LINKLATER Andrew, 31, 32, 63, 191
 LIPSCHUTZ Ronnie, 67, 409
 LITTLE Richard, 394, 448
 LOHARD Audrey, 131, 133
 LONSDALE David, 395, 423
 LOTRINGER Sylvère, 380
 LOUAULT Frédéric, 25
 LOVELUCK Benjamin, 84, 135, 182, 290
 LUCKMANN Thomas, 26
 LUSSAULT Michel, 172
 LYOTARD Jean-François, 378
 MACIVER Robert M, 96
 MACKAY, Hughie, 417
 MACKENZIE Donald, 153, 393
 MACLEOD Alex, 41, 65, 69
 MAISL Herbert,, 315
 MÄKINEIF Saku, 450
 MANESS Ryan, 424, 429, 430
 MANJIKIAN Mary, 390, 395, 448, 451
 MANSFIELD, Edward D, 88
 MARCUSE Herbert, 151, 171
 MARKUS, Gyorgy, 52
 MARTIN Clément, 110, 111
 MARTINEZ William, 90
 MARTIN-LALANDE Patrice, 319
 MARX John, 100
 MASCO Joseph P, 393
 MASOUD Tarek, 47
 MASSIT-FOLLEA Françoise, 301
 MASTERMAN Margaret, 29

- MATTELART Armand, 166
 MAURER Tim, 415
 MAUSS Marcel, 146, 147, 148, 156, 157,
 158, 159, 160, 261, 444
 MAYAFFRE Damon, 87, 88, 89
 McBURNEY Peter, 192, 193
 McCARTHY Daniel, 391, 394, 444, 446
 MCRAE Ronald, 380
 MCSWEENEY Bill, 69, 70, 366
 MEIKLE Graham, 387
 MELMAN Seymour, 380
 MERAND Frédéric, 82
 MEYER Morgan, 101, 273
 MEYET Sylvain,, 56
 MICHAUD Thomas, 133
 MILEO Thierry, 319
 MILLIKEN Jennifer, 53
 MITRA Raja, 415
 MOATI Raoul, 55
 MOL Annemarie, 475
 MOLYNEUX-HODGSON Susan, 101, 273
 MONTGOMERY David, 450
 MORIN Jean-Frédéric, 25
 MOSES Joel, 167
 MUMFORD Lewis, 153
 MURPHY Emma, 412
 MUSSO Pierre, 174, 175, 317
 MUTIMER David, 61
 NAVES Marie-Cécile,, 56
 NEALE Mark, 129
 NEGROPONTE Nicholas, 318
 NEUFELD Mark, 60
 NEUMANN (VON) John, 163
 NEWMAN Abraham, 405
 NEWMYER Jacqueline, 431
 NEXON Daniel H.,, 30
 NICOLAIDIS Kalypso, 103, 277, 278, 282
 NISBET Robert, 164
 NISSENBAUM Helen, 74, 365, 371, 433
 NORA Dominique, 134
 NORTH Robert, 468, 471, 472
 NORTH, Douglass, 416
 NYE Joseph, 12, 393, 396, 419, 420, 423,
 428
 NYSTRAND Martin, 98
 O'MEARA Dan, 41
 O'MIEL Julien, 109
 OGER Claire, 199
 OLLIVIER-YANIV Caroline, 199
 ONUF Nicholas G.,, 38
 PAGANINI Pierluigi, 261
 PAJON Christophe, 110, 111
 PANETTA Leon, 188
 PARFITT Tom, 264
 PARRY Richard, 148
 PASSERON Jean-Claude, 75, 77, 78, 79, 82,
 83, 88, 98, 107, 126, 175, 187, 280, 345,
 361
 PAVE Francis, 354
 PERRIN Jean-François, 75
 PERROTTET Jean-Philippe, 185, 258
 PERSSON Johannes, 46
 PETERSON John, 277, 279
 PETITEVILLE Franck, 57
 PEVEHOUSE Jon., 88
 PFEFFER Jeffrey, 357
 PFEFFER Jürgen, 461, 462, 556
 PIERCE Charles S., 105
 PIERSON Paul, 103, 450
 PILET Jean-Benoit, 25
 PINCH Trevor, 154, 155, 447, 448
 PLATON, 126, 148, 149
 POHL Frederick Julius, 380
 POSSONY Stefan Thomas, 379
 POUILLOT Vincent, 82
 POULIOT Vincent, 101
 POURNELLE Jerry, 379
 PRINCE Daniel, 372
 PROTEVI, John, 452
 PROULX Serge, 168, 182, 444
 QUERE Louis, 444
 RADAELLI Claudio, 85, 276
 RAILTON, Peter, 45
 RAMEL Frédéric, 27, 39, 53, 82, 86, 87, 158,
 273, 289
 RAUS Rachèle, 136
 RAUS Rachèle, 91, 133
 REARDON Robert, 390
 REINERT Max, 197
 REINGOLD Edward, 209
 RHEINGOLD Howard, 132, 144
 RIBEMONT Thomas, 56
 RICŒUR Paul, 50
 RID Thomas, 189, 192, 193, 308, 364
 RIFKIN Jeremy, 381
 RIORTY Richard, 54
 RISSE Thomas, 42, 406
 RIST Gilbert, 57

- ROBERT Pascal,, 315
ROE Emery, 85
ROMANI Roger, 323
ROMANY Roger, 259
RONFELDT David, 146, 308, 309, 381, 382
ROSENAU James, 366, 396
ROSENAU Pauline, 66
ROSENBERG Nathan, 32, 155
ROSENBLUETH Arturo, 137
ROSNAY (DE) Joël, 317
RUGGIE John Gerard,, 279
RUPERT Mark, 445
RUSSETT Bruce, 468
RUTHS Derek, 461, 462, 556
SABATIER Paul, 102, 279
SACO Diana, 366
SAKR Naomi, 413
SALANCIK Gerald, 357
SALOMON Jean.-Jacques, 155
SAMAAN Jean-Loup, 308
SANDAL Nukhet, 273
SANDHOLTZ Wayne,, 73
SAPIN Burton, 37
SCHELL Bernadette, 190
SCHINDLER Sebastian, 457
SCHLANGER Nathan, 146
SCHMEDER Geneviève, 155
SCHMIDT Brian C, 36
SCHMITT Michael, 312
SCHRECKER Cherry, 96
SCHUURMAN Frans, 413
SCHWARTAU Winn, 188
SEARLE John, 55
SEGAL Jérôme, 138, 163
SERRES Alexandre, 144
SFEZ Lucien, 124, 170, 179, 444
SHACKELFORD Scott, 473
SHACKELFORD Scott J, 408, 409
SHACKLEY Simon, 104, 268
SHANNON, Claude, E, 162
SHAPIRO Ian, 47
SIKKINK Katheryn, 38, 73
SIMMONS Beth, 42
SIMONDON Gilbert, 151
SKINNER Quentin, 54, 55
SMELSER Neil J., 270
SMITH Bruce, 308
SMITH Dan, 381
SMITH Rogers, 47
SMITH Steve, 32, 41, 44, 47
SNYDER Richard C, 37
SOUTOU Georges-Henri, 361
SPINETTE-ROSE Marie-Paule, 143
SPINETTE-ROSE Robert, 143
SRNICEK Nick, 451
STERLING Bruce, 130
STEVENS Tim, 141, 473
STONE John, 308
SUAREZ Sandra, 414
SUCHMAN Lucy, 444
SUN TZU, 13
SUSSAN Remi, 135
SWALES, John M., 98
TABER Charles, 460
TAGUIEFF Pierre-Alexandre, 164, 166, 167
TAILLAT Stéphane, 297
TANCZER Leonie Maria, 303
TARDE Gabriel, 160, 161
TARDE Gabriel,, 133
THERY Gérard, 318
THOMPSON Edward Palmer, 381
TIMPONE Richard, 460
TOFFLER Alvin, 144, 382
TOFFLER Heidi, 382
TÖNNIES Ferdinand, 96
TORYN Didier, 182
TUIN (van der) Iris, 451
ÜNVER Akin, 460
VALERIANO Brandon, 424, 429, 430
VAN CREVELD Martin, 381
VAN BOUWE Jeroen, 46
VAN DER PIJL Kees, 445
VAN ZEEBROECK Nicolas, 143
VANDENDORPE Christian, 90
VASSILIOU Marius, 363
VENTRE Daniel, 135, 141, 180, 188, 352,
 422, 423, 426
VERNADSKY Vladimir, 146
VERNADSKY Vladimir, 146
VINGE Vernor, 191
VIPREY Jean-Marie, 89
VIRILIO Paul, 165, 380
VOS POST Jonathan, 140, 380
WÆVER Ole, 41, 67, 68, 73, 366, 373
WALKER John, 184
WALSER Randal, 183
WALTZ Kenneth, 31, 393
WARUSFEL Bertrand, 315

- WEAVER, Warren, 162
WEBER Claude, 185, 258
WEBER Erik, 46
WEBER Max, 60, 97, 299
WEIBLE Christopher M.,, 279
WEINBLUM Sharon, 86
WELDES Jutta, 354, 366
WELLS Herbert George, 345
WENDT Alexander, 38, 42, 47, 392, 447
WENGER Etienne, 102, 273
WESTHOFF Frank, 416, 417
WESTRUM Ron, 153
WIENER Norbert, 137, 139
- WIGHT Colin, 47, 394
WIGHT Martin, 32
WILCOX Lauren, 452
WILDE (DE) Jaap, 67, 73, 366, 373
WILLE Tobias, 457
WILLIAMS Michael Charles, 70
WOOLGAR Steve, 451, 454
WYN JONES Richard, 62
YLIKOSKI Petri, 46, 48
ZALEWSKI Marysia, 41
ZELIKOWV Philip, 361
ZETLAOUI Tiphaine, 144
ZITO Anthony, 275

Titre : Relations Internationales et cyberespace, théories et acteurs asymétriques

Mots clés : Science politique, Relations Internationales, Etudes critiques de sécurité, analyse de discours.

Résumé : Partant du phénomène de la prolifération du « cyberespace » et de l'ensemble des termes qui en sont dérivés, cette thèse interroge la prise en considération de la sécurité de l'information et de son influence sur les Relations Internationales.

Afin de répondre à cette question, cette recherche croise la combinaison pragmatique conduite par les problèmes avec une analyse de discours mobilisant plusieurs approches méthodologiques, notamment la logométrie et les communautés épistémiques.

Parmi ses principaux résultats, cette thèse déconstruit les récits qui entourent le cyberespace de ses origines littéraires à son réemploi dans l'administration. Elle quantifie un accroissement de sa diffusion pour définir un ensemble de préoccupations liées à la sécurité de l'information. Après l'analyse de discours sous l'angle des études critiques de sécurité combinée à l'étude de ses réceptions dans les Théories des Relations Internationales, la thèse propose de comprendre la sécurité de l'information notamment sous l'angle des théories cyberpolitiques de Nazli Choucri, de la théorie de l'acteur-réseau.

Title : International Relations and cyberspace, theories and asymmetric actors

Keywords : Political Science, International Relations, Critical Security Studies, Discourse Analysis.

Abstract : Based on the phenomenon of the proliferation of "cyberspace" and all the terms derived from it, this thesis questions the consideration of the security of information and its influence on International Relations

To answer this question, this research combines problem-driven pragmatism with a discourse analysis involving several methodological approaches, including logometry and epistemic communities.

Among its main results, this thesis deconstructs the narratives that surround cyberspace from its literary origins to its re-employment in administration. It quantifies an increase in its dissemination to define a set of information security concerns. After the analysis of discourse from the angle of Critical Securities Studies combined with the study of its receptions in the Theories of International Relations, the thesis proposes to understand the security of information especially from the angle of the Nazli Choucri's cyberpolitics theories and the actor-network theory.