"Les cyberattaques comme instruments de puissance dans les relations sino-américaines."

HENROT, Guillaume

ABSTRACT

Ce travail de fin d'étude porte sur la thématique du cyberespace et de son statut en tant que théâtre d'opération d'un nouveau type de conflit opposant la Chine et les États-Unis : la cyberguerre. Dans ces conflits, quel rôle les cyberattaques jouent-elles dans la dégradation des relations sino-américaines ? Ce travail va tenter d'apporter des éclaircissements en analysant ces conflits à travers la perspective réaliste des relations internationales.

CITE THIS VERSION

Faculté des sciences économiques, sociales, politiques et de communication
École des sciences politiques et sociales (PSAD)

Les cyberattaques comme instrument de puissance dans les relations sino-américaines.

Auteur : Henrot Guillaume
Promotrice : Van Wynsberghe Caroline
Année académique : 2019-2020
Master en Sciences Politiques, orientation générale

Code de déontologie de l'UCLouvain

« *Je déclare sur l'honneur que ce TFE a été écrit de ma plume, sans avoir sollicité d'aide extérieure illicite, qu'il n'est pas la reprise d'un travail présenté dans une autre institution pour évaluation, et qu'il n'a jamais été publié, en tout ou en partie. Toutes les informations (idées, phrases, graphes, cartes, tableaux, ...) empruntées ou faisant référence à des sources primaires ou secondaires sont référencées adéquatement selon la méthode universitaire en vigueur.*
Je déclare avoir pris connaissance et adhérer au ***Code de déontologie pour les étudiants en matière d'emprunts, de citations et d'exploitation de sources diverses*** *et savoir que le plagiat constitue une faute grave***. »**

HENROT GUILLAUME

Avant-Propos

Avant d'aborder le travail de fin d'étude à proprement parler je tiens à remercier les différentes personnes qui m'ont apporté leur aide lors de ce travail de longue haleine.

Je tiens en premier lieu à remercier Mme Caroline Van Wynsberghe, la promotrice de ce TFE, pour ses conseils, ses remarques. Celles-ci m'ont poussé, à chaque relecture, à approfondir le thème de ce travail un peu loin.

Un grand merci à ceux qui ont pris le temps de relire ce travail et d'apporter leurs remarques. En particulier, je remercie mon père pour ses relectures méticuleuses.

Je voudrais remercier Mme Claudia Di Marzio, secrétaire de la faculté PSAD, pour sa patience et le temps qu'elle m'a consacré lors de mes nombreuses interrogations d'ordres administratives.

Enfin, ce travail est dédié à ma maman, qui nous a quitté en début d'année après un long combat contre la maladie.

Table des matières

Introduction

Afin de choisir un sujet de recherche adéquat pour ce travail, il me paraissait approprié de sélectionner un thème qui gravite autour d'un des domaines qui, d'une part, constitue de grands enjeux à l'heure actuelle et, d'autre part, occupera une place de plus en plus importante dans le futur des relations interétatiques. Il s'agit du concept de cyberespace et, par extension, des cyberinteractions entre plusieurs acteurs. Dans le cadre de ce travail, la question de recherche développée ci-dessous s'orientera vers les différents conflits qui se déroulent au sein du cyberespace et comment ceux–ci impactent les relations entre deux superpuissances, à savoir les États-Unis et la Chine.

Tout d'abord, ce travail de recherche débutera par une mise en contexte qui sera subdivisée en deux parties. D'une part, il y aura un état des lieux des relations diplomatiques entre la République Populaire de Chine et les États-Unis, notamment dans le domaine du cyber. D'autre part, il serait, dès lors, judicieux de mettre en lumière les différentes législations et les différentes doctrines présentes au sein de ces nations. Cette mise en contexte permettra de formuler une question de recherche ainsi que des hypothèses de réponse à celle-ci.

Ensuite, une revue de la littérature permettra d'établir un cadre d'analyse de la problématique étudiée dans ce travail, notamment par le biais d'auteurs comme Mulligan ou Schneider, qui ont contribués à théoriser les doctrines de différentes nations autour du domaine de la cybersécurité. Dans un souci d'apporter un cadre théorique cohérent avec la thématique de recherche, la perspective réaliste des relations internationales sera développée afin de permettre une analyse claire et succincte. Les concepts-clés de cette approche, comme le principe d'anarchie internationale et le principe d'équilibre des puissances théorisés par des auteurs comme Morgenthau et Waltz, seront définis afin d'isoler les éléments applicables à cette problématique. Pour clôturer le cadre de l'analyse, il me paraît judicieux d'aborder de manière plus approfondie les deux hypothèses qui auront été préalablement exprimées. Ainsi, la première hypothèse émettra comme proposition de réponse la recherche d'un statu quo entre les puissances, justifiée par la puissance dissuasive des armes cybernétiques chinoises et américaines. La seconde hypothèse se reposera sur l'idée d'une volonté d'atteindre l'hégémonie dans le cyberespace, où les cyberattaques seraient un moyen d'y accéder.

Le deuxième chapitre de ce travail se concentrera sur l'analyse des hypothèses émises ci-dessus. Cette recherche dressera un état de la situation des nations antagonistes, par le biais d'auteurs comme Mikk Raud et son étude menée pour l'OTAN qui traite du projet d'innovation cybernétique chinois, par exemple. La suite de cette analyse sera focalisée sur le conflit sino-américain, où la perspective réaliste y sera imbriquée. En conclusion de ce chapitre, les résultats de cette recherche analytique seront décrits et expliqués, hypothèse par hypothèse.

La conclusion générale portera, dans un premier temps, sur un rapide récapitulatif de l'évolution de la démarche de recherche, de la question de recherche de départ jusqu'aux résultats obtenus après l'analyse des hypothèses. Dans un second temps, il convient de décrire les limites d'une démarche de recherche ayant pour thème le cyberespace, comme notamment l'intangibilité de ses frontières. Pour terminer, les dernières lignes seront dédiées aux pistes de réflexion résultant de l'analyse effectuée plus tôt. Cette section s'intéressera tout particulièrement à la possibilité –ou non– de transposer des règles de droit international au cyberespace.

1.1 Mise en contexte : historique et législations.

1.1.1 La situation Chine - États-Unis.

À l'heure actuelle, les relations diplomatiques sino-américaines sont plutôt tendues sur plusieurs domaines, principalement au point de vue économiques et politiques. De la guerre commerciale aux tensions en mer de Chine du Sud, il paraît évident que les relations diplomatiques et commerciales entre les deux nations se sont durcies et semblent destinées à perdurer. Cette guerre commerciale initiée par le Président américain Donald Trump se traduit essentiellement par un durcissement des droits de douanes pour l'importation de produits chinois sur le sol américain. Cependant, l'administration Trump tend à rétropédaler comme le prouve l'accord commercial sino-américain signé en janvier 2020.

Il faut également prendre en compte la dimension historique qui lie les deux pays. En effet, les prédécesseurs de Donald Trump ont longtemps et largement contribués à l'émergence de la Chine, alors nation émergente, comme superpuissance économique. Même si la politique agressive des États-Unis est pour le moment sans conséquences directes pour les américains, la puissance économique chinoise et l'extension exponentielle de son influence géopolitique internationale pourraient exposer les futurs présidents américains à de sérieux problèmes avec leurs homologues chinois[1]. De plus, éclatant au début de l'année 2020, la pandémie mondiale du COVID-19 joue un rôle de catalyseur dans la dégradation des relations entre Américains et Chinois. En effet, le coronavirus tient son origine de Wuhan, en Chine. À l'heure actuelle ce sont les États-Unis qui comptent le plus grand nombre de personnes infectées et de morts à cause de ce virus.

Dans ce contexte, l'usage de cyberattaques, comme notamment l'espionnage industriel serait tout à fait envisageable dans le chef des deux camps.

1.1.2 Les différentes législations concernant le domaine du cyber.

En Chine, la première loi sur la cybersécurité a été adoptée par le Congrès National du Peuple chinois en novembre 2016 et est entrée en vigueur en juin 2017[2]. Cette loi représente une avancée fondamentale dans la législation et la gestion de la cybersécurité sur le territoire chinois. Dans les faits, cette loi – appelée *The Cybersecurity Law* – regroupe et synthétise toutes les législations et tous les règlements préexistants à différentes échelles, pour faire émerger des principes structurés applicables à un niveau global. Il est également prévu dans cette loi, des normes pour des problématiques qui pourraient potentiellement se poser sur le long terme. Celles-ci serviront de base juridique quand lesdits problèmes apparaîtront. La loi sur la cybersécurité prévoit également des réglementations et des définitions détaillées sur la responsabilité juridique. Par conséquent, la loi accorde aux autorités chargées de la cybersécurité et de l'administration, des droits et des directives pour l'application de la loi en cas d'actes illégaux.

Aux États-Unis, deux évènements majeurs dans le développement de la législation autour de la cybersécurité ont eu lieu. D'une part, la création en février 2015 d'une nouvelle agence dédiée à la cybersécurité – la CTIIC[3]– par Barack Obama. D'autre part, la mise en place de la directive

[1] VERMANDER, B., *« La Chine et les États-Unis : partenaires et concurrents »,* pp. 453-462.
[2] HONGQUAN, Y., *"Privacy, data protection and cybersecurity law review: China"*, pp. 115-135.
[3] Pour Cyber Threat Intelligence Integration Center (obamawhitehouse.archives.gov)

CISA[4] qui encourage, à l'aide de cadres juridiques, l'échange entre le gouvernement américain et le secteur privé de toutes informations en rapport avec les cybermenaces et les cyberdéfenses[5].

L'actuel Président Donald Trump a fait de la cybersécurité, l'un de ses arguments de campagne en 2016, voulant monter un comité d'experts pour renforcer les mesures déjà opérationnelles. De plus, Le Département de la Défense des États-Unis met à jour régulièrement sa cyberstratégie en y incluant notamment, depuis 2019, l'apport de l'intelligence artificielle et le développement des compétences en matière de cybersécurité.

1.2 La question de recherche.

Cette mise en contexte permet d'établir une question de recherche gravitant autour du cyberespace et mettant en scène deux des plus grandes puissances nationales et internationales : la Chine et les États-Unis.

Pourquoi, depuis 2009, les cyberattaques jouent-elles un rôle toujours plus important en termes de catalyseur dans la dégradation des relations internationales entre les États-Unis et la Chine ?

La date de 2009 paraît être un bon point de départ pour délimiter la question de recherche, car il s'agit de la première année du premier mandat de Barack Obama à la tête des États-Unis. Comme cités plus haut, Obama a mis en place plusieurs politiques et infrastructures innovatrices dans le domaine de la cybersécurité. De plus, le Président actuel, Donald Trump, tend à prendre une direction diamétralement opposée aux politiques de son prédécesseur. Il peut, dès lors, être instructif – du point de vue des répercussions sur la politique internationale – de constater l'évolution des mesures sur une période de dix ans.

Cette question de recherche se focalisera sur les relations Chine – États-Unis. En effet, bien que la Russie soit le concurrent direct des États-Unis dans le domaine du cyber, les relations sino-américaines paraissaient comme idéales pour être traitées dans ce travail de recherche, notamment au vu des récents scandales d'espionnages et des tensions économiques entre les deux pays.

1.3 Les hypothèses pour y répondre.

Pour apporter une réponse à la problématique de recherche, il convient de formuler deux hypothèses de réponse qui seront détaillées plus tard.

La première hypothèse émet l'idée, à l'heure de la numérisation globale, de voir les cyberattaques comme l'équivalent d'une arme – potentiellement– hautement destructrice. Par conséquent, il est nécessaire de les considérer comme une arme de dissuasion dans les relations internationales entre deux grandes puissances, comme la République Populaire de Chine et les États-Unis. Cette menace réciproque mènerait à une neutralisation mutuelle.

La seconde hypothèse serait, dans une perspective réaliste, d'assumer que les cyberattaques soient un moyen pour une grande puissance mondiale de prendre l'ascendant sur son concurrent

[4] Pour Cybersecurity Information Sharing Act

[5] VAKILINIA, I., SENGUPTA, S., *"A coalitional game theory approach for cybersecurity information sharing*", pp. 237-242.

direct. Le but est d'assurer son hégémonie politique et économique. Cela signifierait, par conséquent, que les relations internationales seraient en état de guerre numérique permanente

1.4 La méthodologie de travail.

La méthode employée dans le cadre de ce travail consistera à déterminer le positionnement des différents acteurs aussi bien étatiques que non-étatiques par rapport aux concepts de cybersécurité et de son rôle dans les relations interétatiques.

L'objet de recherche étant assez précis et ciblé, l'utilisation de questionnaire pour une enquête d'opinion me paraît inappropriée car inefficace. Il convient de conduire une recherche à l'aide d'articles scientifiques, de rapports de Think Tanks ou encore de papiers officiels émis par les différents gouvernements et instances internationales afin d'apporter une réponse aux hypothèses qui seront émises. Les conditions particulières, dues au confinement, lors de la rédaction de ce travail ont cependant rendu impossible plusieurs entretiens prévus avec différents experts du domaine du cyber.

2 Chapitre I : Le cadre d'analyse

2.1 Les cyberattaques : la typologie et les cas particuliers des États-Unis et de la Chine.

Afin d'établir un cadre d'analyse cohérent, il paraît judicieux d'établir une typologie des cyberattaques. En effet, selon Nicolas Tenèze[6], il existe douze types de cyberattaques pouvant être répertoriées et distinguées les unes des autres. Cette liste permettra de dégager une définition claire des cyberattaques employées dans les relations diplomatiques entre la Chine et les États-Unis.

Ce tableau ci-dessous reprend les douze types de cyberattaques décrites dans *Combattre les Cyber Agressions*, de Nicolas Tenèze ainsi qu'une brève description.

Type de cyberattaque	Description
Les ADS	Attaque par Déni de Service. Il s'agit d'une attaque qui vise à rendre impossible l'utilisation d'un service (comme un serveur, une boîte mail).
Le cyberespionnage	Infiltre clandestinement les systèmes informatiques d'une organisation ou d'un individu, et à s'emparer de données pour les exploiter.
Le cyberharcèlement	Violence, en particulier psychologique, harcèlement moral ou sexuel, humiliation, intimidation, utilisant Internet comme support
La cyberfraude	Fraude se déroulant sur Internet.
Le cyber-whistleblowing	Regroupe les lanceurs d'alertes utilisant des moyens cybernétiques comme support.
La cybercontrefaçon	Contrefaçon par Internet.
La cyberfinance criminelle	Piratage d'infrastructure financière dans le but de faire du profit.
La cyberpropagande	Propagande effectuée via des canaux de communications du cyberespace.
Le défaçage	Modification non sollicitée de la présentation d'un site web, à la suite du piratage de ce site.
La cyberusurpation d'identité	Vol d'identité subie sur le web, à des fins nuisibles.
Le cybercambriolage	Vol de données effectuée par Internet.

[6] TENEZE, N., « *Combattre les Cyber Agressions : enjeux, politiques et limites* »

Parmi ces différents types de cyberattaques, deux semblent correspondre à la problématique de ce travail et sont d'ailleurs corroborées par Ryan Seebruck dans son ouvrage *Digital Investigation (volume 4).* Il s'agit, d'une part, de l'attaque par déni de services via des logiciels malveillants comme les chevaux de Troie, les spywares ou encore les infecteurs de fichiers et, d'autre part, le cyberespionnage – qui est dans ce cas-ci de nature industrielle. Seebruck apporte, par ailleurs, une précision quant aux motivations se cachant derrière ces cyberattaques. Celles-ci sont au nombre de quatre : la notoriété, la curiosité, l'aspect financier et la vengeance[7]. Ces quatre motivations servent de base à la mise en place d'une typologie de cyberactivistes. Dans *Digital Investigation*, Seebruck reprend les idées émises par Thomas Holt dans *The Attack Dynamics of Political and Religiously Motivated Hackers* [8], pour préciser que les « hacktivistes » peuvent être motivés par des idéaux politiques et/ou religieux [9].

Dans le but de comprendre en quoi ces cyberattaques jouent un rôle toujours plus prépondérant dans les relations diplomatiques entre les États-Unis et la Chine, il paraît important d'aborder les doctrines sur la cybersécurité propre à chaque nation.

2.1.1 Les États-Unis.

Il y a eu en 2015 une grande poussée vers le développement de propositions de lois sur le cyberespace – la dernière datait de 2002, le *Federal Information Security Management Act.* Le but était de rendre le sujet, complexe et abstrait, de la cybersécurité plus compréhensible et concret[10]. Cette nation propose une doctrine sur la cybersécurité qui se base sur une logique d'effets[11]. La question clé qui détermine la manière dont les États-Unis réagiront aux attaques est de savoir quels effets ces dernières vont avoir sur leurs infrastructures. Que les effets résultent de moyens cybernétiques ou physiques importent peu[12]. Des normes naissantes suggèrent que les États-Unis pourraient envisager de promouvoir une réglementation structurée contre les attaques à grande échelle, contre les infrastructures civiles et également d'évaluer les possibilités et l'éventuelle efficacité d'une norme anti-cyberattaques contre les systèmes de commande et de contrôles nucléaires[13]. Cette doctrine semble démontrer que les Américains mettent en avant un système dit « défensif », et que leurs attaques ne se font qu'en réponse à une agression subie par leurs infrastructures.

Il est cependant judicieux de rappeler les divers scandales de ces dernières années. Il y a eu en 2013 les révélations de l'ex-agent de la CIA, Edward Snowden, concernant les écoutes effectuées par les autorités américaines, via des programmes comme GENIE, PRISM ou encore XKeyscore[14]. Cet espionnage s'étendait de collectes d'informations en ligne auprès des

---

[7] SEEBRUCK, R., "*A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model*", pp.38-39.
[8] HOLT, T. J., "*The Attack Dynamics of Political and Religiously Motivated Hackers*", p.159.
[9] SEEBRUCK, R., "*A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model*", p.40.
[10] TRAUTMAN, L., "*Cybersecurity: What about U.S. Policy*", p 341.
[11] MULLIGAN, D., SCHNEIDER, F., *"Doctrine for cybersecurity",* pp.78-80.
[12] FARRELL, H., GLASER, C., "*The role of effects, saliencies and norms in US Cyberwar doctrine*", pp 7–17.
[13] *Ibidem*
[14] VAUDANO, M., *« Plongée dans la 'pieuvre' de la cybersurveillance de la NSA ».*

citoyens américains – à leur insu – à des mises sur écoute d'institutions internationales, comme le Conseil Européen à Bruxelles.

Récemment, en juin 2019, en réaction à la destruction par l'Iran d'un drone américain, Donald Trump a lancé une cyberattaque contre les systèmes de lancement de missiles et un réseau d'espionnage iraniens.

2.1.2 La Chine.

La République Populaire de Chine a reconnu l'existence d'unités dédiées à la cyberdéfense. Selon Daniel Ventre, les forces de cyberdéfense chinoises sont de trois types. Premièrement, les forces militaires spéciales de guerre sur les réseaux qui sont, par conséquent, des unités militarisées. Deuxièmement, des équipes de spécialistes du monde civil – les ministères, par exemple – disposant d'autorisations de l'armée pour mener à bien des opérations de cyberdéfense. Troisièmement, des entités non-étatiques, mobilisables à tout moment, formées et organisées pour de telles opérations[15].

Cette reconnaissance officielle vient conforter les États-Unis et beaucoup d'autres nations qui ont depuis plusieurs années menées des enquêtes sur les cyberattaques, concluant souvent à l'implication des acteurs étatiques chinois. De plus, cela met fin à un certain déni de la part de la Chine, qui a toujours jusque-là nié le soutien des forces armées dans de quelconques cyberattaques, notamment à des fins d'espionnage industriel, comme ce fut le cas avec Huawei sur le sol américain. Pour finir, cela implique la nécessité de repenser les coopérations engagées par la Chine en matière de lutte contre la cybercriminalité. La confiance envers les institutions étatiques chinoises qui d'un côté prétendent lutter contre la cybercriminalité mais qui, d'un autre côté, soutiennent des opérations d'hacking contre les intérêts des États avec lesquels elles coopèrent, se retrouve fortement dégradée à la suite de cette reconnaissance officielle[16].

De plus, Pékin a été accusé par le passé d'attaques qui réduisent au silence les discours politiques en dehors des frontières de la Chine dite « continentale ». En 2014, un référendum informel tenu en ligne concernant l'avenir politique de Hong Kong a engendré ce qui a été considéré comme l'une des plus grandes attaques de ce type de l'histoire. Un an plus tard s'est déroulée une série de cyberattaques ayant pour but de détourner du trafic de Baidu – le moteur de recherche chinois – et ainsi surcharger un site web hébergeant des copies de services bloqués en Chine, comme Google, la BBC et le New York Times.

[15] VENTRE, D., « *A propos de la cyberdéfense chinoise* », Mars 2015.
[16] *Ibidem*

2.2 La perspective réaliste et le cyberespace.

Pour permettre une analyse approfondie autour de cette problématique de recherche, il convient d'en définir les concepts qui y sont rattachés ainsi que la théorie qui sera utilisée plus tard, dans le cadre de l'analyse à proprement parler.

2.2.1 La théorie.

L'analyse du sujet de la recherche se fera sous l'angle du réalisme – aussi appelé la perspective réaliste dans les relations internationales. Cette école a pour principales références Raymond Aron, Kenneth Waltz et Hans Morgenthau.

Cette théorie se concentre sur les conflits et la guerre entre les nations. La guerre, selon Morgenthau, est une conséquence de l'anarchie internationale qui entraîne le déclenchement d'un processus d'auto-défense des États.

Les États, d'ailleurs, sont pour les auteurs réalistes les seuls acteurs habilités pour disposer d'une force coercitive et des autres forces lui permettant d'assurer sa propre sécurité. Cette souveraineté leur garantit à la fois l'absence d'ingérences étrangères dans leur politique nationale et la liberté par rapport aux autres acteurs internationaux[17]. Dans cette course à la puissance et à la souveraineté, les États finissent par se menacer les uns les autres. En effet la question : « Est-ce qu'un État s'arme uniquement pour se défendre ou pour attaquer un État voisin ? » se pose et les différents acteurs entrent dans une course à l'armement sans fin, dans le but de maintenir un équilibre des puissances entre eux.

2.2.2 Les concepts.

Dans le cadre de cette question de recherche, on peut distinguer deux grandes catégories regroupant les concepts. Il y a, d'un côté, les notions liées au domaine du cyberespace et de l'autre, celles gravitant autour de la perspective réaliste dans les relations internationales.

a) Les concepts autour du domaine du cyber.

Tout d'abord, il est essentiel d'apporter une définition au **cyberespace** en tant que tel. Les auteurs de ce domaine d'étude définissent le cyberespace dans le sens premier du mot cybernétique, le cyberespace serait l'espace qui mène l'information. C'est le lieu où sont menées les actions cybernétiques. Ce concept est construit par opposition au monde physique, où ont lieu les actions dites cinétiques. Le cyberespace regroupe toutes les ressources cybernétiques des différents pays. Cela inclut d'une part, les capacités physiques et technologiques, telles que l'Internet et ses instruments, les ordinateurs en réseau, les communications spatiales, et d'autre part, les compétences humaines[18]. Ces ressources, une fois comptabilisées, permettent de définir si une nation acquiert – ou non – le statut de **cyberpuissance**. De plus, le cyberespace étant un terrain nouveau, sans législation claire et

[17]Selon la perspective réaliste, en l'absence d'une grande autorité supérieure, les États sont autonomes et indépendants.

[18] NYE, J., "*The Future of Power in the 21st Century: Cyber Power*", pp.3-8.

dans lequel l'accès à l'information est relativement simple, il est devenu un enjeu de puissance considérable.

Une fois le lieu défini, il faut apporter des éclaircissements sur les actions qui s'y déroulent, les actions **cybernétiques**. Ce terme a été inventé en 1948 par Norbert Wiener pour désigner la science des machines automatiques. Il s'intéressait particulièrement au principe d'autorégulation. Les recherches sur la cybernétique ont contribué à la fondation de l'intelligence artificielle, entre autres. De plus, Wiener a développé la conception selon laquelle l'information et la communication sont absolument nécessaires et vitales au fonctionnement de la société.

Abordons, dès à présent, le type d'actions cybernétiques qui nous intéressent dans le cadre de ce travail, les **cyberattaques**. Celles-ci bénéficient de deux définitions. L'une est donnée par le vice-amiral français et directeur du CICDE[19] , Arnaud de Tarlée. Selon lui, une cyberattaque est « Une action volontaire, offensive ou malveillante, menée au travers du cyberespace et destinée à provoquer un dommage aux informations et aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support »[20]. La seconde provient de l'ANSSI[21], qui assimile les cyberattaques à des « Tentatives d'atteinte à des systèmes d'information réalisées dans un but malveillant. […] elles peuvent avoir pour objectif le vol de données (secrets militaires, diplomatiques ou industriels), détruire, endommager ou altérer le fonctionnement normal de systèmes d'information ».

Pour se protéger contre ce type d'attaque, les États mettent sur pied un autre concept, la **cybersécurité**[22][23]. Il s'agit de la condition optimale recherchée par un système d'information, lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises. Cela s'applique également aux services connexes que ces systèmes offrent ou qu'ils rendent accessibles[24]. Chaque nation a ses propres doctrines en matière de cybersécurité, certaines étant plus agressives que d'autres.

b) Les concepts découlant de la perspective réaliste.

Premièrement, il faut mettre en lumière un des premiers postulats de la perspective réaliste, l'**anarchie**. En effet, avec son livre *Theory of international Politics*, Kenneth Waltz reprend le concept mis au point par Morgenthau et nous apprend que « Le système international est dans un état perpétuel d'anarchie […] l'absence d'autorité centrale signifie que les États doivent veiller à leur sécurité par-dessus tout s'ils ne veulent pas disparaître »[25]. Selon ce concept, il n'y a pas de leader ou d'autorité centrale supérieure qui possède le monopole du pouvoir coercitif et qui ait la légitimité d'en disposer. C'est pourquoi les États, qui sont autonomes et indépendants, se trouvent dans une situation de guerre permanente. Le terme anarchie

[19] Pour Centre Interarmées de Concepts, de Doctrines et d'Expérimentations.
[20] De TARLEE, A., *« glossaire interarmées de terminologie opérationnelle »,* p.51.
[21] Pour Agence Nationale de Sécurité des Systèmes d'Informations.
[22] QUEMENER, M., PINTE, J-P., « *Cybersécurité des acteurs économiques : Risques, réponses stratégiques et juridiques »,* p.241.
[23] JOHANSON, D., "*The Evolving U.S. Cybersecurity Doctrine*", p.37.
[24] De TARLEE, A., *« glossaire interarmées de terminologie opérationnelle »,* p.51.
[25] WALTZ, K., « *Theory of International Politics* », p.102.

représente la distribution décentralisée du pouvoir dans le système international. Cela veut dire qu'il n'y a pas d'organe international tout puissant. Cette conception peut d'ailleurs se transposer au domaine du cyber, où il n'existe aucune réglementation supranationale.

De cette anarchie internationale découle une autre conception, qui est celle de la ***self-help,*** que Waltz définit dans *Theory of International Politics.* Selon lui, « La condition d'anarchie provoque l'incertitude des États sur les intentions des autres : ils ne peuvent compter que sur eux-mêmes »[26]. Cela signifie, quel que soit sa taille ou sa nature, qu'un acteur international doit assurer sa propre protection – ou dans le cas contraire, prendre le risque de subir la puissance d'un autre État. C'est un principe d'auto-défense sous l'anarchie internationale de la perspective réaliste.

Deuxièmement, pour assurer ce principe de *self-help*, les États doivent développer leur **puissance** (ou pouvoir). Le pouvoir des États, du point de la perspective réaliste, ne se soucie que des capacités matérielles sans prendre en compte des facteurs comme l'influence ou les revenus. La puissance d'une nation est trop difficilement mesurable en termes d'intentions ou de revenus. Selon les réalistes, il est préférable de mesurer le pouvoir en termes de matériels ou de capacités – au sein desquelles les capacités militaires et économiques sont primordiales. Kenneth Waltz, le père de la perspective néoréaliste, définit les capacités d'un État en utilisant différentes unités de mesures : « La densité de population, la taille du territoire, la dotation en ressource, la capacité économique, la force militaire et la stabilité politique »[27]. De plus, Morgenthau décrit dans *Politics among Nations* que « Il existe différents déterminants matériels de la puissance : un vaste territoire, une population nombreuse, une économie forte […] »[28]. L'ensemble de ses paramètres définissent le niveau de puissance d'un État par rapport à un autre.

Troisièmement, cette puissance permet aux États d'augmenter leur **souveraineté**, qui représente un attribut de l'État qui montre que ce dernier n'est pas soumis à une plus grande puissance que ce soit à l'étranger ou à l'intérieur de ses frontières. L'État ne doit cependant n'avoir aucune implication dans la juridiction nationale d'autres nations. Ce concept peut être assimilé à une forme de liberté d'action des États dans leurs relations avec les autres.

Quatrièmement, un des concepts principaux de l'école réaliste est **l'équilibre des puissances**[29]. Ce dernier se traduit par une stratégie où chaque État s'assure qu'aucune nation ne domine le système international et ainsi permettre un équilibre instable entre les États. Il ressort de ce principe ce que les auteurs réalistes appellent **le dilemme de sécurité**. Ce dilemme découle du fait que chaque nation amasse du pouvoir dans le but de se protéger à un point qu'elle en devient une menace pour les autres États. Dans son ouvrage *Politics among Nations*, Morgenthau nous permet de comprendre que « les États ne peuvent mener que trois types de politiques rationnelles : maintenir leur puissance, l'augmenter ou la démontrer »[30]. Ces derniers sont, par conséquent, obligés d'augmenter leur propre puissance afin d'assurer leur défense et de

[26] WALTZ, K., « *Theory of International Politics* », p.104
[27] *Ibidem,* p.131.
[28] MORGENTHAU, H., "*Politics among Nations: The Struggle for Power and Peace*", p.26.
[29] NAU, H., « *Perspectives on International Relations: Power, Institutions, and Ideas* », pp.42-50.
[30] MORGENTHAU, H., "*Politics among Nations: The Struggle for Power and Peace*", p.25.

maintenir l'équilibre. On ne peut pas être sûr des motivations des États voisins à propos des raisons qui les poussent à augmenter leur puissance. Ceci entraîne une course à l'armement infinie.

Enfin, il est intéressant de mentionner un dernier concept de la perspective réaliste, l'**hégémonie**. Les défenseurs de la perspective réaliste offensive affirment que les États cherchent à atteindre l'hégémonie, invoquant comme raison que plus de pouvoir vaut mieux que moins de pouvoir. En situation hégémonique, les autres puissances n'ont aucune chance de vaincre la nation dominante. L'hégémonie correspond, par conséquent, à une situation où une nation est plus puissante que les autres nations prises individuellement.

2.3 Les hypothèses en détails.

2.3.1 Première hypothèse : le statu quo entre les puissances.

Pour rappel, la première hypothèse supposait, à l'heure de la numérisation globale, de voir les cyberattaques comme l'équivalent d'une arme – potentiellement– hautement destructrice. Par conséquent, il est nécessaire de la considérer comme une arme de dissuasion dans les relations internationales entre deux grandes puissances, comme la République Populaire de Chine et les États-Unis. Cette menace réciproque mènerait à un statu quo.

Dans le cas de cette proposition, on tente d'expliquer le phénomène en mettant en relation la puissance potentielle d'outils comme les cyberattaques et la neutralisation réciproque qui en découle entre les deux nations étudiées, la Chine et les États-Unis.

Dans une certaine mesure, on peut comparer les armes cybernétiques à l'arme nucléaire en termes de menace qui pèse sur une société. Aujourd'hui, toutes les infrastructures sensibles des plus grandes puissances trouvent leur source et leurs éléments critiques dans le cyberespace. Celles-ci sont, par conséquent, potentiellement vulnérables aux attaques cybernétiques de nations étrangères, voire même d'acteurs non-étatiques comme les hackers.

De la même manière qu'il y a eu une course au nucléaire dans les années 60 – conduisant à une neutralisation mutuelle –, la puissance cybernétique et son potentiel destructeur dans les différents secteurs essentiels constituent une menace réciproque pour le fonctionnement d'un État dans les relations internationales. Cela pourrait, en définitif, mener des nations comme la Chine et les États-Unis à un statu quo.

Dans le cas de cette hypothèse, la force de frappe cybernétique d'une superpuissance est telle qu'une attaque de grande ampleur contre une autre superpuissance entraînerait une escalade de la violence dans le cyberespace. Cette force de frappe agit donc comme un garde-fou mutuel et permet un statu quo.

2.3.2 Deuxième hypothèse : la quête de l'hégémonie.

La seconde hypothèse serait, dans une perspective réaliste, d'assumer que les cyberattaques soient un moyen pour une grande puissance mondiale de prendre l'ascendant sur son concurrent direct. Le but est d'assurer son hégémonie politique et économique. Cela signifierait, par conséquent, que les relations internationales seraient en état de guerre numérique permanente.

Pour cette hypothèse, il s'agit de considérer les cyberattaques utilisées par une superpuissance comme une arme de déstabilisation contre ses adversaires, afin d'assurer son hégémonie politique et/ou économique.

Il est intéressant de constater que les nations impliquées peuvent aussi bien avoir recours à des programmes informatiques nationaux via des agents étatiques qu'à la sollicitation d'agents non-étatiques – comme des entreprises ou des particuliers. La croissance exponentielle des interconnexions des réseaux informatiques indispensables à la vie d'une nation a eu pour conséquence de rendre les pays les plus développés plus vulnérables et plus sensibles aux cyberattaques. Considérés comme le « système nerveux » des États[31], les réseaux informatiques se sont transformés en un enjeu de premier plan pour les différentes nations.

Ici, la compétition dans la prééminence mondiale et internationale est expliquée par le recours à des cyberattaques de la part de superpuissances –comme la Chine et les États-Unis– contre leurs concurrents via des acteurs aussi bien étatiques que non-étatiques. Cela montrerait donc que ces nations se livrent à une guerre de l'information secrète et permanente.

[31] DESFORGES, A., *« Les représentations du cyberespace : un outil géopolitique »,* p. 67.

3 Chapitre II : L'analyse

3.1 L'analyse des hypothèses.

3.1.1 Rappel des hypothèses.

c) L'hypothèse du statu quo.

Comme expliqué dans le cadre d'analyse, la première hypothèse exprimait l'idée que les cyberattaques seraient, dans le contexte actuel international, à considérer comme une arme de dissuasion entre les États – au vu de son potentiel destructeur pour les infrastructures de ces derniers. Cette menace réciproque – et la neutralisation mutuelle qui en résulte – aurait pour but d'établir un équilibre entre les nations.

Dans le cas de cette hypothèse, on cherche à démontrer l'existence d'un statu quo entre les puissances concernées par ce travail de recherche, la Chine et les États-Unis. Dans son ouvrage, *World Politics* – où fut publiée la *Power Transition Theory* –, A.F.K Organski apporte une définition de l'état de statu quo entre les nations. Selon lui, « le statu quo est utilisé pour décrire des États qui considèrent le système international, le droit international et souvent même l'économie de marché comme des aspects à part entière du spectre international qui devraient être respectés »[32]. Par ailleurs, les États en statu quo se reconnaissent en tant que tels et ne sont pas menacés les uns par les autres. Les États devraient, par conséquent, être confrontés à moins de problèmes empêchant une possible coopération interétatique.

Cependant, l'état de statu quo est un équilibre fragile, car il se base sur la confiance envers les autres acteurs internationaux. Il peut donc être facilement rompu, même par des moyens détournés comme des cyberattaques. C'est pourquoi, la neutralisation mutuelle des armes cybernétiques entre les États pourrait poser une garantie dans le maintien d'un statu quo dans les relations sino-américaines.

Pour cette hypothèse, l'existence du statu quo cité ci-dessus s'explique par les cyberattaques et plus particulièrement leur (non-)utilisation. La Chine et les États-Unis font partie des pays les plus actifs en matière de cybersécurité. D'une part, les États-Unis sont bien établis comme cyberpuissance – notamment depuis le premier mandat de Barack Obama. D'autre part, La Chine, bien qu'elle ne soit pas, selon Mikk Raud, une cyberpuissance à proprement parler[33] – à cause de ses défaillances en ressources humaines et de son cadre institutionnel fragile – assure un développement de son expertise cybernétique dans tous les niveaux de la société chinoise (administration, infrastructure, …). Ces deux puissances internationales, selon cette hypothèse, optent pour le maintien de l'équilibre dans leurs relations en maintenant la paix dans le cyberespace.

[32] ORGANSKI, A.F.K.," *World Politics",* p.19.
[33] RAUD, M.," *China and cyber: attitude, strategy and organization*", p.9.

d) L'hypothèse de la quête d'hégémonie.

La seconde hypothèse serait, dans une perspective réaliste, d'assumer que les cyberattaques soient un moyen pour une grande puissance mondiale de prendre l'ascendant sur son concurrent direct. Le but est d'assurer son hégémonie politique et économique. Cela signifierait, par conséquent, que les relations internationales seraient en état de guerre numérique permanente.

Pour cette hypothèse, on cherche à prouver que, au-delà d'un équilibre dans la balance des puissances, c'est l'hégémonie politique et économique qui est recherchée par la Chine et les États-Unis. L'hégémonie se caractérisant par une domination sans partage dans un secteur. Un pays en situation hégémonique représente une menace car il est tellement supérieur aux autres pays pris individuellement qu'il les contraint à s'allier les uns aux autres – et donc à faire des concessions.

Néanmoins, dans *Politics among Nations*, Hans Morgenthau nous permet de comprendre que « La guerre a un rôle dominant et fait partie des forces naturelles et immuables qui ne doivent pas être contrées mais utilisées »[34]. Par cette explication, on peut déduire que l'état d'hégémonie implique un état de guerre permanent. Les nations soumises à une hégémonie, craignant pour leur sécurité et leur souveraineté, vont absolument vouloir neutraliser la suprématie d'une nation pour ramener un équilibre entre les puissances, qui leur sera moins défavorable.

Dans le cas de cette hypothèse, l'objectif d'hégémonie politique et économique recherché par les deux nations concernées s'explique par l'utilisation d'armes cybernétiques. Les États-Unis, leaders mondiaux dans le domaine du cyber, cherchent à conserver leur suprématie et sapent les forces de leurs adversaires. La Chine, une nation qui monte en puissance dans le cyberespace, cherche à renverser le pouvoir établi et prendre sa place.

3.1.2 Rappel théorique.

La théorie utilisée dans ce travail de recherche pour analyser cette piste de réponse sera, pour rappel, le réalisme dans les relations internationales. Les facteurs clés dans l'analyse des hypothèses sous le prisme de cette perspective seront de constater, d'une part, le rôle que joue l'équilibre des puissances dans les relations sino-américaines et, d'autre part, de comprendre l'impact du recours à l'utilisation –ou la non -utilisation– des armes cybernétiques.

3.1.3 Recherche Analytique.

Cette recherche analytique se déroulera en trois parties. Premièrement, les cas de la Chine et des États-Unis seront examinés sous l'angle de la théorie réaliste. Deuxièmement, le conflit sino-américain sera lui aussi étudié. Troisièmement, des résultats seront dégagés de cette recherche et permettront de confirmer, d'infirmer ou encore de nuancer l'hypothèse de recherche concernée.

[34] MORGENTHAU, H., "*Politics among Nations: The Struggle for Power and Peace*", p.3.

e) La Chine.

Pour Pékin, la seule façon de développer ses capacités dans le domaine du cyber devait se faire par une autonomie nationale en innovation, qui nécessite une stratégie elle aussi nationale d'intégration profonde de la cybernétique dans les capacités militaires et civiles[35].

Cette stratégie s'inspire en particulier de celle des États-Unis. Cette inspiration découle d'un double constat de la part des autorités chinoises[36]. En effet, celles-ci observent, d'une part, que les capacités cybernétiques de la Chine sont à la traîne par rapport à celles des Etats-Unis. D'autre part, le système de cyberdéfense américain est souvent cité comme étant un système puissant et efficace. La cybersécurité américaine a été mise en œuvre par un partenariat solide entre les différents secteurs s'occupant de la défense et les industries civiles. Ainsi, Les entreprises privées qui se sont spécialisées dans le domaine informatique et de la cybersécurité fournissent le support technologique et logistique sur lequel reposent les stratégies de l'armée américaine dans le cyberespace. Cette dernière, en contrepartie, soutient, investit et acquiert parfois des entreprises privées.

Le gouvernement chinois a pris conscience de l'importance de l'enjeu que constitue la maîtrise du cyberespace. Premier fournisseur de composants électroniques, la Chine a, par conséquent, choisi d'investir massivement dans les technologies informatiques et cybernétiques tout en développant une « muraille du Net [37]» visant au contrôle de son propre cyberespace national. Par ailleurs, le style d'intégration à l'américaine – reposant sur des accords entre le secteur public et le secteur privé – convient également au modèle économique chinois, où une grande majorité des entreprises sont nationalisées. Cela permettrait de faciliter la coopération entre les entreprises civiles et les structures militaires chinoises.

Ce projet d'incorporation des capacités militaires avec les industries civiles n'est pas nouveau, mais l'ampleur et le rayonnement qu'il prend modifieraient en profondeur le système de protection de cybersécurité chinois. D'un côté, l'industrie de cyberdéfense publique –et par conséquent l'infrastructure militaire qui y est rattachée – souffre d'importants manquements, notamment en termes d'innovation et d'efficacité. Ceux-ci sont, pour la plupart, hérités de l'isolationnisme chinois [38]. D'un autre côté, le secteur privé chinois, qui a connu une progression et une croissance exponentielle pendant près de deux décennies, est aujourd'hui un acteur indispensable au bon fonctionnement de la société chinoise. Les entreprises chinoises contribuent, en effet, à 70 % des innovations techniques et à 65 % des brevets nationaux[39]. Celles-ci disposent par conséquent des ressources pouvant corriger les manquements présentés plus haut des infrastructures militaires publiques.

Mikk Raud nous explique dans son étude pour l'OTAN, *China and cyber : attitude, strategy and organization*, que ce projet de coopération peut se présenter comme une stratégie à trois strates interdépendantes[40]. Premièrement, cette coopération doit privilégier les forces armées et leurs demandes. Deuxièmement, la coopération se passe en coconstruisant et en promouvant les innovations technologiques et cybernétiques. Troisièmement, il est indispensable

[35] LINDSAY, J., "*The Impact of China on Cybersecurity: Fiction and Friction* "pp.10-16.
[36] RAUD, M.," *China and cyber: attitude, strategy and organization*", p.6.
[37] *Ibidem*, pp.6-9.
[38] HJORTDAL, M., "*China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence*", pp. 5-8.
[39] D'après le rapport de l'étude de l'économie chinoise émise par l'OCDE, datant d'avril 2019.
[40] RAUD, M.," *China and cyber: attitude, strategy and organization",* pp.19-24.

d'incorporer pleinement la recherche et le développement, dans le but d'atteindre l'émergence d'une intelligentsia nationale compétente.

D'après les recherches de Magnus Hjortdal dans son ouvrage *China's use of Cyber Warfare,* « L'accélération de l'innovation nationale constitue le point central de la réforme de la politique de cybersécurité chinoise. Le gouvernement de Xi Jinping souhaite étendre les canaux de coopération et de partage des ressources entre les infrastructures militaires et les industries civiles »[41]. Le secteur de la défense pourra ainsi utiliser l'infrastructure de base des réseaux civils pour corriger ses lacunes dans le domaine de la cybernétique. Cette stratégie d'intégration reposera sur des fonds d'investissement tant public que privé, afin de favoriser le transfert de technologies des administrations militaires vers les administrations civiles.

Depuis le lancement de ce projet d'intégration et d'innovation au début des années 2010, la Chine a quasiment comblé son retard sur les États-Unis, en réorganisant – en un court laps de temps– complètement son économie. Ainsi, comme le révèle le rapport Mandiant[42] en 2013, l'Armée Populaire de Chine a mis sur pied une unité spécialisée dans les cyberconflits : l'Unité 61398[43]. Cela démontre, d'un point de vue réaliste, que la Chine veut se mettre au même niveau des autres cyberpuissances et ainsi assurer sa propre souveraineté dans le cyberespace.

En passant cette approche chinoise de la cybersécurité sous le spectre de la théorie réaliste des relations internationales, on peut constater plusieurs éléments. Tout d'abord, la notion d'équilibre des puissances est ici pleinement représentée par la volonté de la Chine de vouloir rattraper son retard sur une autre grande puissance mondiale qui fait figure de leader dans le domaine du cyber, les États-Unis. Dans cette optique, le désir d'acquérir une certaine puissance en termes d'armes cybernétiques et ainsi concurrencer le leader mondial actuel peut définir une volonté de rétablir un équilibre entre les nations.

Ensuite, bien que l'armée soit mobilisée et fasse un usage coercitif de ses capacités cybernétiques, le gouvernement chinois met l'accent sur son secteur privé et ses entreprises pour accumuler de la puissance et ainsi augmenter sa souveraineté dans le cyberespace. Cette puissance qui, d'après la perspective réaliste, se mesure par le biais des moyens matériels et les capacités d'un État. Ce projet d'intégration démontre, par conséquent, une réelle volonté de la part de la Chine d'améliorer son pouvoir afin de maintenir l'équilibre dans la balance des puissances.

f) Les Etats-Unis.

Dans le domaine du cyber, les États-Unis, berceau de l'internet[44], font figure de leader mondial incontestable grâce à leurs différents atouts stratégiques. D'une part, les États-Unis hébergent les principaux codes sources et les plus grandes entreprises du domaine du cyberespace ainsi que les infrastructures essentielles au fonctionnement de l'internet mondial, comme les serveurs et les câbles informatiques, par exemple. D'autre part, les révélations du lanceur d'alerte Edward Snowden à propos des différentes écoutes de la part de la NSA ont démontré la capacité et le rayon d'action des États-Unis dans ce domaine, étant donné que l'agence américaine intercepte la quasi-entièreté du trafic internet dans le monde.

[41] HJORTDAL, M., "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", p.9.
[42] Il s'agit du nom d'une société américaine spécialisée dans la sécurité informatique.
[43] Unité avec des tâches semblables à la NSA, dont les actions sont ciblées en Amérique du Nord.
[44] FARRELL, H., GLASER, C., "The role of effects, saliencies and norms in US Cyberwar doctrine", p.8.

En effet, les États-Unis ont mis le cyberespace – et par conséquent la cybersécurité et la cyber-guerre – au sommet de leur agenda stratégique. Washington a décidé, en 2009, de créer un centre de commandement militaire : l'US Cyber Command, qui compte à l'heure actuelle plus de 6 000 experts [45]. Un an plus tard, le gouvernement américain prévient qu'il « […] répondrait à des actes hostiles dans le cyberespace comme il le ferait pour n'importe quelle menace contre leur pays »[46]. On peut constater que les États-Unis prennent donc très au sérieux les cybermenaces. Certains dirigeants américains considèrent aujourd'hui le risque cyber comme plus important que le risque terroriste.

Cependant entre 2015 et 2018, Washington a changé son fusil d'épaule[47]. En effet, il est désormais nécessaire d'avoir une cyberstratégie offensive car cela constitue l'une des clés d'une prise au sérieux à l'international. Cette transition a eu lieu notamment lors du changement de présidence entre Obama et Trump. Ce dernier prône une approche plus agressive de l'utilisation de cyber. Plus la puissance de feu est intimidante et dissuasive, plus on est assuré que le discours sera pris au sérieux au niveau des relations internationales. Une autre conséquence de ce changement de présidence fut la dégradation des relations entre les États-Unis et la Chine. Comme déjà explicité plus haut, Donald Trump a durci les relations sino-américaines, particulièrement au niveau du commerce avec des droits de douanes revus à la hausse. Ainsi, les États-Unis analysent les cybercapacités de nuisance de la Chine avec beaucoup d'attention, car la progression fulgurante de ces dernières au cours des dernières années tend à remettre en cause la suprématie américaine dans le domaine du cyber. On peut constater que les États-Unis et la Chine se distinguent donc par leur avance en matière de cybersécurité – et par extension de cyberguerre.

Du point de vue de la théorie réaliste, la situation des États-Unis, jusqu'au début des 2010, s'apparente à un état de suprématie, d'hégémonie dans le cyberespace[48]. En effet, jusqu'à la réorientation économique de la Russie et de la Chine vers des investissements dans le secteur du cyber, Washington faisait figure d'autorité incontestée et incontestable dans ce domaine.

Bien qu'étant le leader mondial dans le cyberespace, les États-Unis ont décidé, depuis 2018, de transformer leur conception de la cybersécurité en une vision nettement plus agressive[49], notamment à la suite de plusieurs révélations d'espionnage industriel de la part d'entreprises chinoises – en particulier la société de téléphonie Huawei. Ce changement d'idéologie a renforcé le déséquilibre dans l'équilibre des puissances de l'ordre international. En effet, comme l'explique Kenneth Waltz dans *Theory of International Politics*, si la nation dominante renforce sa sécurité, les autres nations sont obligées de renforcer à leur tour leur propre sécurité pour éviter de se faire conquérir[50]. Cela peut mener à une escalade à la fois des armes cybernétiques et à la fois de la violence dans le cyberespace, représentée par les cyberattaques.

[45] WILDAY, T., "Comparing and Contrasting How the United States and China Address Cybersecurity", pp.21-25
[46] *Ibidem*
[47] FARRELL, H., GLASER, C., "*The role of effects, saliencies and norms in US Cyberwar doctrine"*, p.12.
[48] MULLIGAN, D., SCHNEIDER, F., "Doctrine for cybersecurity", pp.70-92.
[49] "*National Cyber Strategy of the United States of America",* pp. 6-11.
[50] WALTZ, K., « *Theory of International Politics* », p.105.

g) Le conflit sino-américain.

Avant toute chose, il faut se rendre compte que, factuellement, chacun de ces États tente de favoriser ses propres entreprises dans le grand marché mondial. Comme l'explique Morgenthau « il existe différents déterminants matériels de la puissance : un vaste territoire, une population nombreuse, une économie forte […] »[51]. Par conséquent, le droit, l'économie, la diplomatie et donc le cyberespace sont autant de domaines dans lesquels l'influence d'un État permet à ses entreprises d'avoir l'avantage et, en finalité, contribuer à la prospérité du pays. Cette conception vient de la notion de l'anarchie au niveau international telle que décrite par Waltz dans Theory *of International Politics*[52]. En l'absence d'autorité supérieure, chaque État cherche à favoriser ses propres entreprises, dans la perspective d'accroitre sa puissance.

Pendant que les différentes institutions peinent à établir des règles et un cadre juridique international du cyberespace, deux États s'y affrontent : les États-Unis et la Chine. Comme nous l'apprend Daniel Ventre dans *Cyberattaque et Cyberdéfense*, les États ont pris conscience du potentiel grandissant des armes cybernétiques reflété par l'affaire estonienne[53][54]. Les Américains et les Chinois ont progressivement élaboré leurs doctrines de cyberguerre, mais aussi des organisations, procédures et armes particulières, comme vu plus haut.

Les États-Unis auraient, en effet, alloué en 2013 un budget de 4,7 milliards de dollars[55] – soit une hausse de 20% par rapport à l'année précédente – destiné au développement de la cyberdéfense et de la cyberguerre. Avec le premier budget militaire au monde et des entreprises performantes dans le domaine du cyber, les États-Unis ont indéniablement une grande puissance de feu en termes de cybernétique. En conséquence, on assiste dès 2009 – soit le premier mandat de Barack Obama – à la création d'un sous-commandement spécifique : l'US cyber command. Le gouvernement américain entreprend en parallèle la construction du plus grand centre de collectes et d'analyses de données informatiques au monde pour un coût de 2,5 milliards de dollars[56]. Ce complexe de bâtiments autosuffisants devrait participer à maintenir la supériorité américaine dans le domaine de l'espionnage et du cyberespionnage. Cependant, le gouvernement américain craint l'inéluctable montée en puissance de son concurrent chinois comme cyberpuissance. C'est pourquoi, la Chine est au centre de l'attention des services de cyberdéfense américains.

Par ailleurs, il existe différents rapports parlementaires du Congrès américain –comme le rapport Northrop Grumman[57] ou le rapport Mandiant – qui pointent les risques d'infiltration par des systèmes d'espionnage chinois via les puces et les circuits intégrés importés[58] aux États-

[51] MORGENTHAU, H., "*Politics among Nations: The Struggle for Power and Peace*", p.26.
[52] WALTZ, K., « *Theory of International Politics* », p.102.
[53] L'Estonie, un des pays les plus connectés au monde, a été victime de cyberattaques massives venant de Russie, ce qui a eu pour conséquence de paralyser l'administration publique du pays, non-protégée.
[54] VENTRE, D., "*Cyberattaque et Cyberdéfense* », p.92.
[55] PONTZ Zach, "US inscreases cyberwarfare budget by 20%".
[56] *Ibidem*
[57] Northrop Grumman Corporation est un conglomérat américain dont les activités gravitent autour de la défense.
[58] KREKEL, B., *"Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation"*, pp. 59-67.

Unis. Des virus seraient ainsi intégrés au firmware[59] et formeraient des « portes dérobées » qui permettraient d'espionner l'utilisateur.

Pour rappel, la cyberstratégie américaine de l'administration Obama était originellement de nature défensive. La posture américaine a changé en 2017 avec l'accession à la présidence de Donald Trump. Avec des visées de suprématie, cette nouvelle cyberstratégie prône des actions pro-actives, quasiment offensives vis-à-vis de ses adversaires, et particulièrement la Chine[60]. La différence de ton dans les cyberstratégies militaires entre les administrations Obama et Trump agit comme un effet miroir à la montée des tensions entre les États-Unis et la Chine.

Du côté chinois, le pays peut compter sur le troisième département de l'Armée Populaire de Chine –dont dépendrait l'Unité 61398 citée plus haut–, les forces spécialisées de sécurité intérieure dans le domaine du cyber et certaines entreprises civiles spécialisées. Pour concurrencer les États-Unis, Pékin a créé, en 2015, l'équivalent de l'US Cyber Command : le Strategic Support Force[61]. Sa tâche est de regrouper les moyens de l'armée dans le domaine de la guerre dans le cyberespace, spatiale et électronique.

Bien que les États-Unis aient été les premiers à avoir investi le cyberespace à un niveau national, Jon Lindsay, dans son livre *China and Cybersecurity : Espionage, Strategy, and Politics in the Digital Domain*, avance le fait que la Chine s'est transformée en concurrent sérieux, voire même en un adversaire potentiellement supérieur aux États-Unis sur deux plans : la population et son contrôle et la maîtrise des composants électroniques[62].

Ainsi, les moyens mis en œuvre dans des actions de cyberguerre se sont considérablement développés chez les deux protagonistes. L'un voulant préserver sa suprématie, l'autre voulant s'en emparer. Les cas d'espionnages et de cyberattaques entre les deux pays se sont multipliés à un point que le conflit a lentement évolué vers une « guerre froide 2.0. »[63]. À la manière de la première guerre froide entre l'Union Soviétique et les États-Unis, cette guerre froide ne fait pas, ou peu, de morts et génère une crispation générale dans les relations diplomatiques internationales. En effet, un accord passé avec l'un des deux protagonistes risque de détériorer les relations avec l'autre.

Au-delà du domaine, militaire, cette nouvelle « guerre froide » repose sur deux bases. D'un côté, les intérêts économiques où il faut constater que, depuis 2012, plus de 80 % des affaires d'espionnage économique effectué contre les entreprises américaines seraient liées à la Chine[64]. D'un autre côté, les deux protagonistes mettent l'accent sur la recherche et le développement dans les domaines de la collecte de renseignements, des sabotages et des opérations d'influence[65]. Cette dernière et la déstabilisation sont également des objectifs importants. La Chine a mis sur pied en 2010 la cyberopération « Aurora » et a visé plus d'une trentaine d'entreprises américaines, dont les mastodontes Dow Chemical et Google. Cet acte, perçu

[59] C'est un programme intégré à un matériel informatique qui lui permet de fonctionner. Ce terme peut se traduire par micrologiciel.
[60] FARRELL, H., GLASER, C., "*The role of effects, saliencies and norms in US Cyberwar doctrine"*, p.13.
[61] LINDSAY, J., "*China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*", p.188.
[62] *Ibidem*, p.51.
[63] Dans le sens où celle-ci se déroule dans le cyberespace, et non plus dans le monde physique.
[64] HUNGERFORD, N., "Chinese theft of trade secrets on the rise, the US Justice Department warns"
[65] GOMPERT, D., LIBICKI, M., "Cyber Warfare and Sino-American Crisis Instability", pp.12-14.

comme une démonstration de force de la part de la Chine, a largement contribué à la détérioration des relations diplomatiques américano-chinoises.

Il convient de préciser que, contrairement à la précédente guerre froide, celle-ci ne prend pas en compte les idéologies politiques des deux protagonistes, bien que ces dernières soient pourtant par nature opposées. En effet, les États-Unis et leur *American way of life* représentent la société capitaliste par excellence, alors que la Chine emploie un modèle communiste avec un contrôle quasi-total de sa population. Ces différences idéologiques ne jouent pas le rôle de moteur dans ce cyberconflit, contrairement aux précédents conflits entre puissances mondiales.

Durant les guerres passées, l'idéologie jouait un rôle prépondérant, notamment dans la perception du conflit par la population. On peut prendre l'exemple de la montée du nazisme dans l'Allemagne des années 1930, où l'idéologie antisémite était omniprésente. Il y eut également le conflit de la Guerre Froide, qui opposa deux blocs aux idéologies diamétralement opposées. Durant ce conflit, il y avait d'après ce que rapporte Jean-Robert Rougé dans son livre *L'anticommunisme aux Etats-Unis de 1946 à 1954*, une véritable « chasse aux communistes » sur le sol américain[66]. Dans le nouveau type de conflit que génère le cyberespace, où les actions sont menées de manières détournées et secrètes, le recours à l'idéologie pour s'assurer le soutien de la population n'est plus indispensable[67]. De plus, on ne cherche plus à vaincre un État à cause de son identité ou de ses valeurs. On pense dorénavant la guerre entre États en termes de marchés et de concurrence commerciale.

Il faut cependant remarquer qu'il existe une grande différence entre les conflits dits « classiques » et le conflit qui a lieu à l'heure actuelle dans le cyberespace entre la Chine et les États-Unis. Il s'agit du statut de l'agresseur et de celui de l'agressé. Lors d'un conflit ouvert, d'une guerre physique, deux armées s'affrontent dans le but de vaincre l'autre et/ou d'obtenir des avantages stratégiques – il faut aussi prendre en compte la volonté d'influer sur le moral de l'adversaire. Le concept de cyberespace renverse cette conception classique des conflits. En effet, le cyberespace n'ayant pas de frontières palpables et ne disposant pas de législation supranationale, le conflit se déplace. La cible n'est plus l'armée adverse mais les structures économiques. Par conséquent, lors d'une cyberattaque, un État ne s'en prend pas de manière directe à un autre État, mais à ses entreprises, ses administrations.

Le rôle de l'agresseur ne subit pas de réel changement car ce sont toujours des États qui attaquent –ou des acteurs-non-étatiques représentant un État. Cependant, les victimes sont maintenant des entités du secteur privé qui doivent se défendre seules. Ce nouveau paradigme transforme la vision de la guerre. Il devient donc nécessaire pour les gouvernements de développer un « art de la cyberguerre », dans le but de préserver leur secteur privé.

[66] ROUGÉ, J-R. « *L'anticommunisme aux Etats-Unis de 1946 à 1954* », p.157.
[67] WILDAY, T., *"Comparing and Contrasting How the United States and China Address Cybersecurity",* pp 6-11.

3.2 Les résultats de la recherche analytique.

3.2.1 La première hypothèse.

À la lumière de la recherche menée ci-dessus, on peut déduire que l'hypothèse selon laquelle les cyberattaques seraient, dans le contexte actuel international, à considérer comme une arme de dissuasion entre les États et que cette menace réciproque aurait pour but d'établir un équilibre entre les nations est à infirmer. Ce rejet de l'hypothèse de recherche est dû à deux raisons majeures.

La première raison est le lieu où se déroule le conflit. Effectivement, le cyberespace est un espace qui n'est ni régulé ni soumis à diverses législations –à un niveau supranational en tous les cas. Cela en fait un espace opaque, qui est plus secret que le monde physique, où il est difficile d'anticiper les actions des autres États. Cette opacité nécessite de faire reposer les relations internationales sur la confiance. Dès lors, il devient complexe d'y construire des relations diplomatiques. Dans ces conditions, il n'y a aucun moyen d'assurer la viabilité de l'équilibre des puissances car chaque nation va renforcer sa propre cybersécurité et développer son cyberarmement jusqu'à atteindre le concept de dilemme de sécurité, tel que décrit par Morgenthau dans *Politics among Nations*[68]. On ne peut pas, effectivement, être certain des motivations des États voisins sur les raisons de leur renforcement dans le domaine du cyber. Ceci entraîne une course à l'armement infinie

La seconde raison est la nature du conflit. Comme vu plus haut, il ne s'agit pas d'un conflit entre un envahisseur et un envahi. Les règles de guerre classiques n'ont aucune emprise dans le cyberespace, il ne s'agit plus d'un État affrontant un autre État rival pour des ressources ou par idéologie. Le cyberconflit sino-américain est avant tout commercial où les cibles privilégiées sont les secteurs privés. De plus, le cyberespace rend flou l'identification des assaillants ; il peut aussi bien s'agir d'unités gouvernementales spécialisées que d'entreprises privées au service d'un gouvernement. Ainsi, les États ont de plus en plus recours à des acteurs à priori non-étatiques, comme ce fut le cas avec l'espionnage industriel mené par Huawei, pour le compte du gouvernement chinois.

En définitive, la course à l'armement cybernétique couplée à l'illisibilité des différents acteurs du conflit annihile une possible confiance entre la Chine et les États-Unis, et par conséquent toute idée de statu quo. C'est pourquoi cette hypothèse est infirmée.

3.2.2 La deuxième hypothèse.

En prenant compte de ce qu'il ressort de la recherche effectuée, on peut statuer que la seconde hypothèse selon laquelle, il faudrait, dans une perspective réaliste, traiter les cyberattaques comme un moyen pour une grande puissance mondiale de prendre l'ascendant sur son concurrent direct est confirmée.

La validation de cette hypothèse découle de plusieurs constats. En premier lieu, il y a la notion d'hégémonie et comment elle est abordée dans le conflit. En effet, ce concept de la perspective réaliste offensive décrit une situation où les autres puissances n'ont aucune chance de vaincre

[68] MORGENTHAU, H., "*Politics among Nations: The Struggle for Power and Peace*", p.25.

la nation dominante individuellement. Cela les contraint, par conséquent, à nouer des alliances pour préserver leur souveraineté. Dans le cas de ce conflit, les États-Unis sont en situation d'hégémonie dans le domaine du cyberespace, et la Chine aspire à atteindre cet état de suprématie. Cette cyberguerre oppose ainsi une nation hégémonique qui veut le rester, à une nation émergente – du point de vue du domaine du cyber – qui désire s'en emparer. Le cœur du conflit est bien la suprématie d'une part cybernétique, d'autre part économique.

Dans un second temps, il faut prendre en compte le rôle des cyberattaques. La recherche a permis de constater que la puissance de dissuasion des armes cybernétiques ne peut pas être comparée à celles des ogives nucléaires. En effet, comme les États ne cherchent pas à maintenir l'équilibre des puissances dans le cyberespace, le recours aux cyberattaques n'est pas rare et fait partie intégrante des relations dans le cyberespace. Loin d'être une arme de dissuasion, l'arme cybernétique constitue un véritable arsenal numérique pleinement utilisable. Il suffit de constater le nombre et les fréquences de cyberattaques lancées ou subies par des nations sur une année[69] pour se rendre compte que les cyberattaques ont été complétement assimilées à l'éventail offensif effectif d'un État.

En conclusion, la dimension hégémonique du conflit et l'usage des cyberattaques dans le cyberconflit opposant la Chine aux États-Unis démontrent que ces derniers ont entamé une guerre non pas dissuasive, mais bel et bien avec des intentions de domination. Cela prouve, par conséquent, que l'hypothèse est validée.

[69] Pour l'année 2014, on a recensé 42,8 millions de cyber-attaques dans le monde soit l'équivalent de 117 339 attaques par jour.

4 Conclusion

4.1 Bref récapitulatif de la démarche de recherche.

Pour rappel, la problématique de recherche cherchait à comprendre pourquoi, depuis 2009, les cyberattaques jouent-elles un rôle toujours plus important en termes de catalyseur dans la dégradation des relations internationales entre les États-Unis et la Chine ?

Pour tenter d'apporter une réponse, deux hypothèses ont été formulées. La première soumettait l'idée que selon laquelle les cyberattaques seraient, dans le contexte actuel international, à considérer comme une arme de dissuasion entre les États et que cette menace réciproque aurait pour but d'établir un équilibre entre les nations. La seconde, quant à elle, proposait, dans une perspective réaliste, d'assumer que les cyberattaques soient un moyen pour une grande puissance mondiale de prendre l'ascendant sur son concurrent direct. Le but est d'assurer son hégémonie politique et économique. Cela signifierait, par conséquent, que les relations internationales seraient en état de guerre numérique permanente.

Ces hypothèses ont été analysées d'une part, sous le prisme de la perspective réaliste. Pour rappel, cette approche décrit les États, comme les seuls acteurs habilités pour disposer d'une force coercitive et des autres forces lui permettant d'assurer sa propre sécurité. Cette souveraineté leur garantit à la fois l'absence d'ingérences étrangères dans leur politique nationale et la liberté par rapport aux autres acteurs internationaux. Les interrogations qui se cachent derrière le renforcement d'un État les poussent à se menacer les uns les autres, ce qui les conduit à une course à l'armement sans fin, dans le but de maintenir un équilibre des puissances entre eux. D'autre part, une recherche empirique a été menée dans le but d'apporter des éléments d'explications qui permettraient de formuler une réponse à ces hypothèses. Cette recherche empirique s'est intéressée au conflit sino-américain et aux doctrines de cybersécurités mobilisées par les deux nations.

4.2 Les résultats de la recherche en bref.

Cette démarche scientifique a abouti à des résultats permettant d'apporter une réponse à la problématique de départ.

Tout d'abord, cette recherche a permis d'écarter la piste de la volonté de la part des deux nations concernées de préserver un équilibre, un statu quo, entre les nations sur le plan du cyberespace. En effet, la course à l'armement cybernétique entre la Chine et les États-Unis additionnée à la non-lisibilité des différents acteurs impliqués dans ce conflit rend impossible toute forme de confiance entre les deux pays, et par conséquent tout projet de statu quo.

Ensuite, il y a un point en particulier qui est ressorti de la démarche de recherche, il s'agit de la dimension hégémonique du conflit. Dans le cas de ce conflit, les États-Unis sont en situation d'hégémonie dans le domaine du cyberespace, et la Chine aspire à atteindre cet état de suprématie. Ce paramètre ajouté à l'utilisation des cyberattaques – qui ne sont donc pas des armes de dissuasion – dans le cyberconflit opposant la Chine aux États-Unis démontre que ces derniers ont entamé une guerre avec des intentions de domination.

Enfin, en recoupant ces différents éléments, on parvient à dresser une réponse à la question de recherche. Si, depuis 2009, les cyberattaques –et par extension le cyberespace– jouent un rôle toujours plus important en termes de catalyseurs dans la dégradation des relations sino-américaines, c'est parce qu'elles constituent un véritable arsenal dans le cyberespace, où se déroule une cyberguerre opposant la Chine aux États-Unis. Ce conflit représente un énorme enjeu au niveau politique, puisqu'il y est question de la domination du cyberespace international. Au niveau économique, l'espionnage industriel permettrait une avancée commerciale dans les marchés étrangers–notamment le marché européen, cible des entreprises américaines et chinoises.

4.3 Limites d'une démarche autour du cyberespace.

Il existe cependant plusieurs limites à la démarche de recherche autour de cette thématique mais la plus importante est sans conteste le cyberespace. Cet espace est, par essence, intangible et invisible. Il est dès lors impossible d'en définir les frontières ni de voir ce qu'il s'y passe. On ne peut, par conséquent, que s'appuyer sur les articles scientifiques rédigés par des entreprises spécialisées or ces dernières sont généralement[70] proches du gouvernement en place. Cela peut biaiser le jugement des auteurs. Il n'a pas toujours été évident de démêler l'opinion politique des rapports purement factuels. En outre, l'absence de législation internationale dans le cyberespace rend impossible la possibilité de se reposer sur un texte de lois et de définir une forme de légalité –ou d'illégalité– de certaines actions dans les relations internationales présentes dans le cyberespace.

La cyberguerre a longtemps été qualifiée de « guerre secrète ». Le sujet étant relativement nébuleux et vaste, il est quasiment impossible de retracer, à la manière d'un historien, l'origine du conflit. De plus ce type de conflit fait appel à des acteurs non-étatiques, il faut dès lors être capable de différencier un agent non-étatique agissant au nom de son pays d'un agent non-étatique totalement indépendant. Cette frontière est d'autant plus floue dans le cas d'un conflit ayant des enjeux commerciaux.

4.4 Vers un droit international transposable au cyberespace ?

Il y a plusieurs pistes qu'il me paraît intéressant de creuser. Une en particulier, étant donné les travaux qui sont menés à l'heure actuelle, mérite d'être développée ci-dessous.

Cet angle de réflexion consiste en l'idée de mettre sur pied des projets de législations ou de réglementations du cyberespace à l'échelle internationale. Les États pourraient s'appuyer sur des textes de droit international fondamentaux comme les conventions de Genève en droit international humanitaire. Il existe aussi des traités internationaux spécialisés concernant les espaces, et également des manuels militaires doctrinaux sur l'emploi des forces.

On peut constater que les sources de droit permettant de répondre aux menaces dans le cyberespace sont nombreuses[71]. Il existe d'ailleurs le Manuel de Tallinn qui est un guide ayant pour but de transposer le droit international dans le cyberespace et plus précisément aux cyberguerres. Ce manuel, qui a vu le jour à la suite de l'affaire estonienne de 2007, n'a cependant aucune valeur juridique et n'est, par conséquent, pas contraignant.

[70] C'est particulièrement vrai pour les entreprises américaines.
[71] BARAT-GINIES, O., « Existe-t-il un droit international du cyberespace ? », pp. 201-220.

Néanmoins, malgré l'absence de volonté de la part des États de création de nouvelles normes internationales spécifiquement destinées au cyberespace et aux cyberconflits, le jeu d'analyse et de mise en lumière de règle de droit national propre à chaque pays face aux attaques cybernétiques reflète, malgré tout, l'intérêt stratégique du domaine pour chaque État[72].

Cette piste de réflexion permet de conclure ce travail de recherche sur le rôle du cyberespace dans les relations interétatiques avec une ouverture sur les perspectives d'avenir d'un espace débordant d'interactions, et pourtant invisible.

[72] BARAT-GINIES, O., *« Existe-t-il un droit international du cyberespace ? »,* pp. 201-220.

Bibliographies

BARAT-GINIES, O., *« Existe-t-il un droit international du cyberespace ? »,* Hérodote, vol. 152-153, no. 1, 2014, pp. 201-220.

DESFORGES, A., *« Les représentations du cyberespace : un outil géopolitique »*, Hérodote, vol. 152-153, no. 1, 2014, pp. 67-81.

De TARLEE, A., *« glossaire interarmées de terminologie opérationnelle »,* N° 212/DEF/CICDE/NP du 16 décembre 2013, p.51.

FARRELL, H., GLASER, C., "*The role of effects, saliencies and norms in US Cyberwar doctrine"*, Journal of Cybersecurity, Vol 3, Issue 1, March 2017, pp 7–17.

GOMPERT, D., LIBICKI, M., "*Cyber Warfare and Sino-American Crisis Instability*", Survival, Vol 56, Issue 4, 2014, pp.7-22.

HJORTDAL, M., "*China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence*", Journal of Strategic Security, Vol. 4, No. 2, Strategic Security in the Cyber Age, 2011, pp. 1-24.

HOLT, Thomas J., "*The Attack Dynamics of Political and Religiously Motivated Hackers*", Proceedings of the Cyber Infrastructure Protection Conference, City University of New York, 2009, p.159.

HONGQUAN, Y., *"Privacy, data protection and cybersecurity law review: China"*, Ed. The Law Reviews, 6th edition, October 2019, pp. 115-135.

HUNGERFORD, N., "*Chinese theft of trade secrets on the rise, the US Justice Department warns*", CNBC,22/09/2019.

JOHANSON, D., "*The Evolving U.S. Cybersecurity Doctrine*", Security Index: A Russian Journal on International Security, Vol. 19, Issue 4, 2013, pp37-50.

KREKEL, B., *"Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation"*, Northrop Grumman Corporation, October 2009, 82p.

LINDSAY, J., "*The Impact of China on Cybersecurity: Fiction and Friction*", International Security, Vol. 39, Issue 3, Winter 2014/15, pp 7-47.

LINDSAY, J., *"China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain",* Oxford University Press, 2 March 2015, 352 p.

MULLIGAN, D., SCHNEIDER, F., *"Doctrine for cybersecurity",* Daedalus, Vol. 140, Issue 4, 2011, pp.70-92.

MORGENTHAU, H., "*Politics among Nations: The Struggle for Power and Peace*", Mc Graw-Hill, 6th ed., New York, 1993, 752p.

"National Cyber Strategy of the United States of America", September 2018.

NAU, H., « *Perspectives on International Relations: Power, Institutions, and Ideas* », Ed. SAGE CQPress, 6th edition, 2019, pp.42-50.

NYE, J., "*The Future of Power in the 21st Century: Cyber Power*", Public Affairs Press, 2011, pp3-8.

ORGANSKI, A.F.K.," World *Politics*", Random House, 2nd edition, 1968, 461p.

PONTZ, Z., *"US inscreases cyberwarfare budget by 20%"*, The Algemeiner Journal, April 2013.

QUEMENER, M., PINTE, J-P., *« Cybersécurité des acteurs économiques : Risques, réponses stratégiques et juridiques »*, Ed. Hermès Sciences publications, coll. « cyberconflits et cybercriminalité », Paris, 13/12/2012, 239p.

RAUD, M.," *China and cyber : attitude, strategy and organization",* NATO CCD COE, Tallinn 2016, 34p.

ROUGÉ, J-R. « *L'anticommunisme aux Etats-Unis de 1946 à 1954* », Presse Paris Sorbonne, 1995, p.157.

SEEBRUCK, R., "*A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model",* Digital Investigation, Vol.4, September 2015, pp36-45.

TENEZE, N., « *Combattre les Cyber Agressions : enjeux, politiques et limites* », NUVIS Editions, Janvier 2018, 578p.

TRAUTMAN, L., "*Cybersecurity: What about U.S. Policy",* Journal of Law, Technology and Policy, Vol. 341, January 2015.

VAKILINIA, I., SENGUPTA, S., *"A coalitional game theory approach for cybersecurity information sharing*" MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, 2017, pp. 237-242.

VAUGHN, R., "*The History of Chinese Cybersecurity: Current Effects on Chinese Society Economy, and Foreign Relations",* Seton Hall University Dissertations and Theses, 2016.

VAUDANO, M., *« Plongée dans la 'pieuvre' de la cybersurveillance de la NSA »*, Le Monde, 27/08/13, mis à jour le 04/07/19.

VENTRE, D., « *A propos de la cyberdéfense chinoise* », Chaire Cyber-Défense et Cyber-sécurité, Mars 2015.

VENTRE, D., « *Cyberattaque et Cyberdéfense* », Éd. Lavoisier, 2011,312p.

VERMANDER, B,. *« La Chine et les États-Unis : partenaires et concurrents »*, Études, vol. tome 399, no. 11, 2003, pp. 453-462.

WALTZ, K., « *Theory of International Politics* », New York: Random House, 1979, 209p.

WILDAY, T., *"Comparing and Contrasting How the United States and China Address Cybersecurity",* Utica College, ProQuest Dissertations Publishing, 2018.

Ce travail de fin d'étude porte sur la thématique du cyberespace et de son rôle en tant que théâtre d'opération d'un nouveau type de conflit opposant la Chine et les États-Unis : la cyberguerre. Dans ces conflits, quels sont les impacts des cyberattaques dans la dégradation des relations sino-américaines ?

Mots-clés : cybersécurité, cyberespace, réalisme, Chine, États-Unis.

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
Faculté des sciences économiques, sociales, politiques et de communication
École des sciences politiques et sociales (PSAD)
Place Montesquieu, 1 bte L2.08.05, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/psad**