Université de Technologie de Troyes

Master en Ingénierie et Management en Sécurité Globale Appliquée

Mémoire de fin d'étude

L'occupation du cyberespace par des groupes terroristes

Damien Clair-Victor

20 décembre 2020

Encadré par Guillaume Delatour, Paul-Henri Richard et Patrick Laclémence
Semestre Automne 2020

Résumé

Titre : L'occupation du cyberespace par des groupes terroristes

Auteur : Damien Clair-Victor

Date de publication : 20 décembre 2020

Mots clés : Cyberterrorisme - Cyberdjiadisme - Cyberguerre - Cyberespace - Cyberopération - Cyber - Terrorisme - Propagande - Guerre d'informations - Défense - Guerre hybride

Résumé : Le cyberespace offre un nouveau domaine d'action au groupes terroristes. Cette étude propose de dresser un panorama sur le champ des possibilités dans le cyberespace pour les groupes terroristes. Il sera ainsi étudié les notions de cyberterrorisme et de cyberdjihadisme. Le cyberespace est également un nouveau domaine comparable aux domaines traditionnels (terre, air, mer) qui se retrouve impliqué dans la guerre contre des groupes terroristes. Ainsi, l'étude portera également sur la guerre hybride qui amène la guerre jusqu'au cyberespace.

Abstract

Title : The occupation of cyberspace by terrorist groups

Autor : Damien Clair-Victor

Date of publication : December 20, 2020

Key words : Cyberterrorism - Cyberjiadism - Cyberwar - Cyberspace - Cyberoperation - Cyber - Terrorism - Propaganda - Information warfare - Defense - Hybrid war

Abstract : Cyberspace offers a new field of action for terrorist groups. This study proposes to draw up a panorama on the field of possibilities in cyberspace for terrorist groups. It will study the notions of cyberterrorism and cyberjihadism. Cyberspace is also a new field like other traditional field (land, air, sea) which finds itself involved in the war against terrorist groups. Thus, the study will also focus on hybrid warfare which brings war to cyberspace.

Table des matières

Table des figures

Table des sigles et abréviations

AIS : Automatic Identification System *(Système d'identification automatique)*
ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information.
C2 : Command and Control
C4 : Command, Control, Communication and Computer
C4ISR : Command, Control, Communication, Computern, Intelligence, Surveillance and Reconnaissance
C4ISTAR : Computerized Command, Control, Communications, Intelligence, Surveillance, Target Acquisition and Reconnaissance
CEMA : Chef d'État-Major des Armées
COMCYBER : Commandement de Cyberdéfense
DIC : Disponibilité, Intégrité, Confidentialité
ETA : Euskadi Ta Askatasun *(Pays basque et liberté)*
FAA : Federal Aviation Administration *(Administration fédérale d'aviation)*
FDI : Frégate de Défense Intermédiaire.
FLNC : Front de Libération Nationale Corse
ICANN : Internet Corporation for Assigned Names and Number *(Coorporation pour l'assignation des adresses sur l'internet)*
L2I : Lutte Informatique d'Influence.
LID : Lutte Informatique Défensive
LIO : Lutte Informatique Offensive
NRBC : Nucléaire, Radiologique, Biologique, Chimique
OIV : Opérateur d'Importance Vitale
OTAN : Organisation du Taité de l'Atlantique Nord
PIV : Point d'Importance Vitale
PSY OPS : Opération Psychologique
QPC : Question Prioritaire de Constitutionnalité
RPK : République Populaire de Donets
RPL : République Populaire de Lougansk

"L'arme cyber est une arme d'emploi. Il n'est plus temps de tergiverser sur l'opportunité de s'en doter ou non. Elle doit être perçue comme un amplificateur des effets militaires traditionnels."

Général d'armée François Lecointre, Chef d'État-Major des Armées, 2019.

Chapitre 1

Introduction

1.1 Motivation et objectif

Ce choix de sujet a été comme une évidence pour moi. Je tenais à y intégrer mes connaissances acquises au cours de ma formation initiale d'ingénieur en réseaux et télécommunications, et plus particulièrement sur ma filière portant sur la sécurité des systèmes et des communications, d'où l'aspect cyber dans ce sujet. Le cyberespace est en effet un domaine passionnant en perpétuelle mutation, avec de multiples enjeux en termes d'économie, d'information et de sécurité.

J'ai grandi en France, loin de tout conflit armé. Cependant, j'ai grandi dans un pays craignant des attaques de groupes terroristes sur son sol et visant sa population. Cette crainte était visible dès mon plus jeune âge par la présence de militaires dans le cadre du plan Vigipirate, mais également par le choc des populations au lendemain du 11 septembre 2001. J'ai également connu durant mon adolescence les attentats de 2015 (Charlie Hebdo, Bataclan) et de 2016 (Nice), qui m'ont particulièrement marqué. Le terrorisme est donc un domaine que je cherche à comprendre pour pouvoir un jour, je l'espère, mieux le combattre par mon travail.

La fusion des domaines terroriste et cyber m'est venue à l'esprit en repensant aux vastes opérations de propagande entreprises par l'État islamique et les prétendues cyberattaques qu'il aurait menées. Travailler sur l'occupation du cyberespace par des groupes terroristes me permet par conséquent de traiter un sujet faisant le lien entre mes deux domaines de formation (cybersécurité et sécurité globale) et mes domaines d'intérêts.

Ce mémoire a pour objectif de me forger une certaine expertise vis-à-vis du sujet choisi afin de consolider mon projet professionnel. Ainsi, souhaitant travailler dans le domaine de la défense, je pense que traiter un tel sujet pourra m'être utile et bénéfique dans mon avenir professionnel.

1.2 Contexte

Depuis les années 2000, la grande majorité des attentats commis sur le sol français sont attribués à des groupes séparatistes, en grande majorité le Front de Libération Nationale Corse (FLNC). Cependant, d'un point de vue médiatique et public, la majorité de ces attentats sont perçus comme des faits divers et non relevant du terrorisme. En effet, en France, l'action des groupes séparatistes est en général axée vers les institutions locales et non contre les civils à l'échelle nationale.

Les actes terroristes perturbant grandement l'ordre public et pouvant aller jusqu'à déstabiliser l'organisation des services de l'État sont quant à eux attribués aux groupes islamiques, en particulier à l'État Islamique ces dernières années. Ces actes se caractérisent par une violence inouïe envers une population bien souvent civile, entrainant un grand nombre de morts.

Nous observons ces dernières années une augmentation des attentats islamistes ; ainsi, entre 2001 et 2015, 232 Français en sont morts en France ou à l'étranger, contre plus de 255 entre 2015 et 2019 avec des attentats de très grande ampleur (attentats de Charlie Hebdo, de Montrouge et de l'Hyper-Cacher faisant 17 victimes en janvier 2015, 13 novembre 2015 entrainant la mort de 130 personnes ou encore Nice en 2016 provoquant 86 morts). Par leurs modes opératoires sanglants (fusillade de masse, véhicule bélier) ces attentats ont profondément choqué et marqué la population française et suscité des réactions à l'international, à l'image de la marche réunissant plusieurs chefs d'États au lendemain de l'attentat de Charlie Hebdo afin de défendre la liberté d'expression. Le profil des victimes a également suscité l'émoi auprès de la population, notamment chez les plus jeunes après les attentats du 13 novembre, où la moyenne d'âge des victimes n'était que de 35 ans. Ces attentats de grande ampleur n'arrachent pas seulement des vies ; ils attaquent les symboles de notre République, ajoutant un choc supplémentaire (liberté d'expression, mode de vie occidental avec ses bars et ses salles de fêtes, fête nationale).

En parallèle de ces attentats très meurtriers, nous avons vu émerger des actes de terrorisme dits « low cost ». Le terrorisme low cost consiste à utiliser des objets communs et à les détourner de leur but (couteau de cuisine, voiture bélier). Ainsi, nous avons vu augmenter le nombre d'attaques au couteau dans la rue visant les civils et les représentants de l'État (en particulier les militaires de l'opération Sentinelle). Ces attentats, moins marquants, alimentent néanmoins la crainte perpétuelle d'un nouvel attentat étant donné la forte place qu'ils occupent dans les médias lorsqu'ils surgissent.[1]

L'apparition du terrorisme low cost en France concorde avec l'importante présence de l'État islamique sur le cyberespace. Au travers des réseaux sociaux, composante majeure du cyberespace « grand public », l'État islamique a en effet passé de nombreux appels au passage à l'acte envers ses sympathisants qui ne pouvaient par rejoindre les combats sur le front en Syrie ou en Irak. [2] La propagande post attentat et le fait

d'ériger le terroriste en martyr permet également de jouer sur le principe du mimétisme afin que de nouvelles attaques spontanées soient réalisées. De plus, grâce à des sites et blogs sur Internet, les groupes terroristes sont parvenus à transmettre des conseils sur la réalisation d'un attentat.

Le développement rapide et continuel du cyberespace mais également de la place qu'il prend dans nos sociétés (l'accès à Internet et aux outils numériques étant de plus en plus étendu à l'échelle planétaire) semble donc être un nouveau terrain propice aux groupes terroristes. De ce constat, se pose alors la question des nouveaux risques et menaces terroristes pesant sur le cyberespace. En effet, le champ des possibilités sur le cyberespace est bien plus vaste qu'une utilisation pour les uniques objectifs de propagande.

1.3 Problématisation

1.3.1 Le cyberespace

Apparu au début des années 1980 sous la plume de William Gibson, fondateur du genre littéraire cyberpunk, le cyberespace est un terme encore mal défini aujourd'hui. Il tire son origine de l'anglais « cyberspace » (contraction des termes « cybernétique », correspondant à l'étude des mécanismes d'information et des systèmes complexes, et « espace » qui représente une étendue abstraite ou non). [3] Au sein du grand public, le cyberespace correspond généralement à l'Internet.

Bien qu'aucun consensus ne se soit dégagé quant à la définition du cyberespace, il apparait que celui-ci s'articule autour de l'idée d'un univers virtuel issu de l'interconnexion mondiale des appareils de système d'information et de communication. L'univers virtuel que représente le cyberespace se base avant tout sur un univers physique ; terminaux d'accès (ordinateurs, smartphones, tablettes, objets connectés...), infrastructures réseaux (antennes, câbles, satellites...), datacenters abritant plusieurs centaines de serveurs hébergeant les différents services du cyberespace. Ce dernier est donc ancré dans le monde physique.[4]

De cette base physique, le cyberespace constitue un environnement de circulation de données numériques permettant l'interaction entre les individus, qui peuvent alors véhiculer de l'information et des idées presqu'en temps réel. Nous assistons également aujourd'hui à l'interconnexion de services automatisés, programmés pour exécuter des tâches plus vite que les individus grâce au traitement massif de données en des temps records (big datas et intelligence artificielle au service des échanges boursiers par exemple).

Le cyberespace permet d'assurer divers services ancrés dans notre société. Par exemple, l'économie, de plus en plus dématérialisée, se base sur le cyberespace (bourse, transactions bancaires, émergence des cryptomonnaies). Ensuite, d'un point de vue

opérationnel, de nombreuses entreprises ou institutions publiques ont des systèmes d'information qui fonctionnent de façon interconnectée. La perte d'interconnexion (qu'elle soit accidentelle ou fruit d'une cyberattaque) leur est en général très préjudiciable et peut les rendre inopérants. Enfin, le cyberespace nous entoure dans notre quotidien avec l'augmentation des objets connectés qui envahissent notre quotidien (smart cities, domotique, secteur médical...).

Il est commun d'aborder le cyberespace selon le modèle de couches proposé par Martin Libicki en 2007. [5] Ce modèle contient 5 couches et chacune des couches du dessus à besoin des couches inférieures pour fonctionner :

- La couche *physique* : composée de serveurs, de câbles, d'ordinateurs, etc. C'est la couche de base supportant le cyberespace.
- La couche *syntaxique* : formée par les protocoles et normes. Sans cette couche, l'interconnexion physique ne mène à rien et les composants ne peuvent pas communiquer.
- La couche *sémantique* : cette couche, plus abstraite, est composée des données du cyberespace et des fonctions d'administration au niveau utilisateur.
- La couche de *services* : on retrouve ici les services accessibles depuis les réseaux qui puisent dans les données disponibles (sites web, services bancaires...).
- La couche *cognitive* : ce sont les interprétations et réceptions des informations issues des services par les utilisateurs.

Cependant, dans le cadre de l'étude menée, ce modèle relativement complet peut être simplifié en trois couches :

- La couche *physique*, conformément au modèle proposé par Libicki.
- La couche *logique* composé de la couche syntaxique, sémantique et de service du précédent modèle.
- La couche *psycho-cognitive* qui garde le même sens que la couche cognitive de Libicki.

La fusion des trois couches du modèle de Libicki en une seule permet de s'affranchir de l'aspect très technique et étroitement lié de celles-ci. De plus, dans le cadre de l'étude menée, il n'y a que peu d'intérêt à scinder cette couche logique ; les interactions possibles étant étroitement liées et du même domaine de compétence. Ce même modèle en trois couches est également mentionné dans la doctrine publique concernant la lutte informatique offensive du ministère des Armées publiée en 2019.[6] Les trois couches sont extrêmement interdépendantes, l'action sur l'une d'entre elles a bien souvent des répercussions sur les autres, notamment dans le sens descendant (action sur la couche physique impactant la couche logique par exemple).

En termes d'utilisation et d'interaction, la couche physique concerne la mise en place de réseaux et d'infrastructures (construction de datacenters par exemple). Pour la couche logique, les utilisateurs peuvent interagir en développant des applications et

en traitant des données. Enfin, concernant la couche psycho-cognitive, les interactions concernent les actions des utilisateurs sur les applications, la communication et la génération d'information ainsi que l'influence recherchée auprès des autres utilisateurs du fait de la réalisation de ces actions.

Nous ne pouvons parler du cyberespace sans prendre en compte sa sécurité. En cybersécurité, il est commun de parler des critères *DIC* : *disponibilité* (capacité du système à être opérable), *intégrité* (assurer la non-modification, la pérennité et l'exactitude des données) et *confidentialité* des données (ne pas être l'objet d'une fuite d'informations). Ces critères sont valables pour l'ensemble des sous-systèmes composant le cyberespace.[7] Les trois couches du modèle précédemment exposé sont soumises à des menaces pouvant altérer un ou plusieurs de ces critères :

- Couche physique : lla destruction des infrastructures (câbles coupés, atteinte d'un datacenter, brouillage d'ondes...) impacte la disponibilité du système et l'intégrité des données (perte de données).
- Couche logique : une cyberattaque peut impacter l'ensemble des critères (virus bloquant un système, virus modifiant les données du système ou qui les efface, backdoor permettant de faire sortir des informations confidentielles).
- Couche psycho-cognitive : cette dernière n'est pas directement liée aux critères DIC mais permet notamment à des personnes malveillantes de mener des opérations de propagande, de revendiquer d'éventuelles actions entreprises sur les couches inférieures ou bien de commanditer des actions (attaques d'infrastructures, cyberattaques). C'est également la perception d'informations qui permet à des individus malveillants d'entrer dans un système d'information (ingénierie sociale).

Sur le cyberespace, par sa nature transfrontalière et abstraite, aucun acteur n'a un contrôle total, contrairement à un État qui serait souverain sur son territoire. La question de la gouvernance du cyberespace consiste alors à identifier le rôle des acteurs, ou plutôt des groupes d'acteurs, et du pouvoir qu'ils ont sur les différentes couches du cyberespace.

- Les instances de standardisation, composées d'utilisateurs bénévoles, d'experts d'entreprises et de chercheurs qui spécifient et définissent les composants des réseaux, des protocoles et des spécifications. Par leur gouvernance technique, juridique et normative ils agissent essentiellement sur la couche logique et sur la mise en place et les conditions de déploiement de la couche physique.
- Les instance de coordination et de gestion, à l'image de l'Internet Corporation for Assigned Names and Number (ICANN) qui attribue les adresses IP sur Internet, gèrent les ressources du cyberespace. Ils agissent donc sur la couche logique.
- Les opérateurs d'infrastructures, tels que les gestionnaires de câbles sous-marins, ont un pouvoir parfois très grand sur la couche physique. Ce sont eux qui sont à la base de la construction physique du cyberespace et de la

connexion des utilisateurs entre eux.

— Les fournisseurs de services, par leurs diverses offres dont certaines sont devenues incontournables, exercent un pouvoir sur la couche logique (proposition de services) et informationnelle (contrôle des données transitant via leur service). Parmi les acteurs de ce groupe, nous retrouvons les membres du GAFAM (Google, Amazon, Facebook, Apple, Microsoft) et à l'échelle asiatique sont équivalentes des entreprises chinoises, le BATX (Baidu, Alibaba, Tencent, Xiaomi).

Le pouvoir de ces acteurs non étatiquse a depuis le début intéressé les gouvernements, notamment celui des États-Unis d'Amérique. Le cyberespace est en effet un domaine aux multiples enjeux pour les États. La recherche du pouvoir de contrôle sur le cyberespace se traduit par l'implication des pays dans les instances de standardisation et de coordination afin de défendre leurs intérêts. Les États veillent notamment à l'implication des opérateurs d'infrastructures et de leurs liens avec des gouvernements pouvant être jugés comme hostiles (par exemple l'opérateur Huawei au travers des antennes 5G aux États-Unis d'Amérique). Enfin, au niveau des opérateurs de services, les États s'inquiètent et s'insurgent parfois d'acteurs étrangers qui traitent les données de leurs citoyens. C'est ainsi que l'Europe a mis en place le Règlement Général pour la Protection des Données (RGPD) afin de s'assurer, entre autres, du bon traitement des données des Européens par les acteurs du GAFAM. Les États peuvent également être sources d'ingérence, à l'image de l'affaire Snowden en 2013 et de l'espionnage de masse entrepris par les États-Unis d'Amérique.[8]

Le cyberespace est un nouveau domaine stratégique pour les États. Ainsi, la France s'est dotée début 2019 d'une doctrine défensive et offensive dans le cyberespace, dans laquelle elle estime que *« « la capacité à conduire des opérations militaires défensives et offensives dans le cyberespace contribue à garantir la souveraineté nationale » [Élément publics de doctrine militaire de lutte informatique offensive, commandement de cyberdéfense (COMCYBER), 2019].*. Bien que ces doctrines soient essentiellement portées envers d'autres acteurs étatiques, elles démontrent l'importance de la maîtrise du cyberespace afin de protéger les intérêts de l'État (protection des infrastructures physiques, résilience face aux cyberattaques, capacité de détecter et limiter la désorganisation par une propagande ennemie).

1.3.2 Les groupes terroristes

Le mot *terrorisme* est apparu au lendemain de la Révolution française afin de désigner les partisans de la Terreur qui menait une lutte envers les contre-révolutionnaires. C'est au cours du XIX^{ème} siècle que le mot terrorisme a commencé à désigner une action contre l'État. Aujourd'hui, le terme terroriste est utilisé à des fins accusatoires très graves, enlevant alors toute légitimité à l'acte.

La définition du terrorisme ne dépend d'aucune convention internationale. Ainsi, malgré tous ses efforts, l'organisation des Nations Unies ne parvient pas à établir une convention contre le terrorisme, qui est une notion différente d'un État à l'autre et qui dépend de la politique du pays. En France, sont considérés comme actes terroristes les infractions basées sur des crimes et délits de droit commun lorsqu'ils sont commis *« en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur » [Article 421-1 du Code Pénal]*. La définition française est donc relativement large ; elle ne se limite pas seulement aux objectifs politiques ou aux attaques contre les civils.[9]

Pour la suite, nous considérerons qu'un groupe terroriste est une entreprise collective, plus ou moins organisée et/ou hiérarchisée, réunissant un ensemble d'individus partageant le même objectif. Ils chercheront à atteindre cet objectif par tous les moyens, y compris délictuels et/ou criminels, qui instaureront un climat de terreur auprès des cibles, aussi bien civiles qu'institutionnelles. Les actions menées ont pour vocation de susciter des réactions émotionnelles vives. Nous retiendrons également que l'objectif est généralement d'ordre politique par les effets de déstabilisation auprès des pays qui sont recherchés au travers des attentats. Enfin, la notion de terroriste agissant en loup solitaire ne sera pas abordée ; c'est en effet une notion de plus en plus sujette à débat sur son existence. Les études tendent à démontrer que les individus sont membres d'un réseau (groupe) en amont et sont seuls uniquement dans l'attaque.

Le cas du terrorisme islamiste

Le terrorisme islamiste (ou djihadiste) concerne les attentats ou actes de terreur commis par des individus, ou plus généralement des membres de groupes islamistes. L'islamisme est une pensée selon laquelle l'islam, deuxième religion dans le monde en termes de pratiquants, devrait guider l'action politique des États. Selon l'islamisme, les États devraient appliquer la charia qui régit un ensemble de règles sociales, culturelles et relationnelles. Cependant, cela irait à l'encontre des droits de l'homme en termes de liberté de croyance, d'expression, mais également en termes d'égalité en ce qui concerne la liberté des femmes.

Le terrorisme islamiste est rattaché à la notion de « djihad » qui représente l'effort que les musulmans doivent fournir au quotidien afin de rester dans le droit chemin de Dieu. Le djihad implique également de combattre les ennemis de l'islam. Le terrorisme islamiste se base donc sur la dernière composante du djihad en prônant que leurs actions ne sont que l'application stricte du djihad et de l'idée de guerre sainte qui en découle.

L'État islamique

L'État islamique a vu le jour en Irak en 2006, à la suite du désordre géopolitique engendré par la guerre d'Irak de 2003. Il se considérait alors comme étant le gouvernement légitime du pays. Courant 2012, l'État islamique a pu s'étendre au-delà de l'Irak avec la guerre civile syrienne. En 2014, l'État islamique proclame un calife, terme

désignant le successeur du prophète, qui règne alors sur le califat, correspondant aux territoires et populations qui l'occupent, conquis lors des guerres.

Entre 2014 et 2015, l'État Islamique prospère et étend ses territoires. Il se substitue pleinement aux États sur les territoires conquis. Il applique alors la charia, met en place une police, une administration, s'approprie et exploite les ressources telles que le pétrole, etc. En 2014, l'État islamique rentre en conflit avec Al-Qaïda et augmente son influence sur le monde musulman, avec l'allégeance de groupes terroristes islamistes à l'étranger (Boko Haram sévissant au Nigeria par exemple).

C'est à partir de 2015 que le groupe terroriste se fait particulièrement connaitre en Occident au travers d'attentats. Contrairement aux attentats organisés par Al-Qaida, l'État Islamique frappe des cibles diverses et pas forcément symboliques. Il s'approprie également des attentats qu'il n'a pas forcément organisés, tel l'attentat de Nice en 2016, pour peu qu'ils aient entretenu des relations avec l'auteur.

Cependant, depuis 2015, l'État islamique connait une série de défaites militaires à la suite de l'importante coalition internationale visant à le combattre. Le territoire de l'organisation terroriste s'est considérablement réduit et les villes les plus stratégiques telles que Raqqa, leur ancien quartier général, ont été reprises (voir annexe A - Évolution des territoires de l'État islamique). Cependant, les territoires reconquis sont anéantis et non viables (villes complètement détruites, présence de mines ou autres pièges). Les années de conflits et la destruction des villes sont à l'origine d'un désastre humanitaire et source d'importants déplacements de populations, notamment vers l'Europe. L'État islamique a profité de ces flux migratoires pour faire rentrer des terroristes sur le sol européen afin d'y perpétrer des attentats.

De nombreux pays considèrent l'État islamique comme une organisation terroriste. L'Union Européenne ainsi que les Nations Unies accusent le groupe d'être responsable de génocide et de nettoyage ethnique envers les Kurdes ainsi que de crimes de guerre et de crimes contre l'humanité (esclavage, viol, torture...). L'organisation terroriste est également à l'origine de la destruction et du pillage de nombreux vestiges archéologiques dans les zones conquises.

L'État islamique a marqué la communauté internationale par l'utilisation de vidéos filmant leurs atrocités à des fins de propagande. Ces vidéos concernent notamment des exécutions d'otages d'une violence inouïe (soldats brulés vifs, noyés, décapités, écrasés par un char d'assaut...). L'utilisation des réseaux sociaux a également permis aux groupes terroristes de recruter de nouveaux combattants en Occident et/ou de les pousser à commettre un attentat directement dans leur pays.[10]

Le cas du terrorisme séparatiste

L'objectif poursuivi par les séparatistes est de se détacher d'un État. Les membres d'un groupe terroriste séparatiste revendiquent alors la gouvernance d'un territoire géographique par des actions parfois violentes (attentats, assassinats). La France a

été confrontée au terrorisme séparatiste, notamment dans les régions Corse (FLNC) et Bretagne (Gwenn ha du), ainsi que dans moindre mesure dans le Pays Basque (ETA). Ces mouvements ont été peu meurtriers en France. Aujourd'hui ces groupes ont été dissouts et la France n'est plus confrontée au terrorisme séparatiste, bien que l'idéologie indépendantiste subsiste chez certaines parties de la population dans ces régions.

Au niveau international, le terrorisme séparatiste se retrouve principalement sous forme de guerres, telles que les guerres opposant les séparatistes tchétchènes et l'armée russe. Lors de ces guerres, des attentats particulièrement marquants ont été perpétrés par des terroristes séparatistes tchétchènes, à l'image de la prise d'otages d'une école dans la ville de Beslan en Russie, entrainant la mort de 334 civils dont 186 enfants.[11]

Le conflit israélo-palestinien est également un exemple de terrorisme séparatiste depuis les accords d'Oslo. Les attentats envers Israël sont en effet nombreux (attentats-suicides, attaques au couteau, tirs de roquettes) sur fond d'un conflit lié à l'occupation des terres. Le terrorisme palestinien est à l'origine de plus de 4 000 morts en Israël, majoritairement civils. Il est également à l'origine de plus de 2 000 morts du côté des civils palestiniens. [12] Néanmoins, les attentats ne relèvent pas uniquement du séparatisme mais également de l'islamisme, avec notamment des groupes, tels que le Hamas, qui se revendiquent comme étant nationalistes religieux.[13]

Dans un dernier exemple lié à la scène internationale, nous pouvons citer celui de la crise Ukrainienne de 2013 qui a déclenché l'émergence de groupes séparatistes (jugés comme étant terroristes par l'Ukraine) pro-russes tels que la République Populaire de Donetsk (RPK) ou la République Populaire de Lougansk (RPL). Lors de la guerre du Donbass, des conflits armés ont pris place entre l'armée ukrainienne et les groupes séparatistes sur le territoire ukrainien. La guerre du Donbass est à l'origine d'au moins 15 000 morts, dont plus de 3 000 civils. Ces conflits ont été source d'exactions envers les populations civiles jugées pro-ukrainiennes. [14] Les conflits ont également détérioré les conditions de vie et sont source de crises humanitaires et sanitaires des populations.[15]

Bien que la France n'ait connu aucun attentat majeur ou conflit armé lié à des groupes séparatistes, ces derniers sont à l'origine de plusieurs milliers de morts au cours de ces dernières années dans le monde. À l'échelle européenne, ils sont également la source des derniers conflits armés se déroulant sur le sol européen.

1.3.3 Problématique

Dans un pays souverain, le gouvernement dispose d'outils efficaces (services de renseignement pour mener une enquête, police qui peut intervenir...) afin de lutter contre les groupes terroristes sur son territoire. Sur le cyberespace, relativement vaste, les problématiques de gouvernance prennent le dessus et complexifient cette lutte. L'intervention pour faire cesser un acte relevant du terrorisme peut ne pas être possible. Pour illustrer ce point, prenons l'exemple d'un site de propagande hébergé sur un serveur à l'étranger qui ne reconnaitra pas l'action comme relevant d'un acte de propagande terroriste (divergence des définitions du terrorisme).

Les groupes terroristes peuvent donc profiter de ce manque de moyens d'action et de coordination entre les États afin de s'installer et profiter pleinement du cyberespace, à commencer par la propagande. Cependant, comme nous l'avons vu, il est également possible de mener des actions lourdes de conséquences sur le cyberespace et de porter atteinte aux intérêts d'un pays. Les groupes terroristes cherchant à provoquer des pertes humaines peuvent ainsi utiliser ce nouveau domaine pour y mener des cyberattaques engendrant les pertes humaines. Dans le cadre de la guerre contre le terrorisme, le cyberespace peut servir à des fins de soutien à leurs opérations traditionnelles. La guerre contre le terrorisme semble donc pouvoir subir une mutation du fait de l'utilisation du cyberespace.

À partir de ces constats peuvent se poser les questions suivantes :

— Quelles sont les formes actuelles de l'occupation du cyberespace par des groupes terroristes ?

— Comment s'intègre le cyberespace dans la guerre contre le terrorisme ?

Le premier axe tentera de répondre à la première question en se focalisant notamment sur les groupes terroristes islamistes tels que l'État islamique. Afin de définir les formes de l'occupation du cyberespace par des groupes terroristes, l'étude portera sur la compréhension de concepts y afférent tels que le cyberterrorisme et le cyberdjihadisme. Enfin, l'objectif sera de déterminer, notamment au travers d'une étude de cas sur l'attentat islamiste de Conflans-Sainte-Honorine, les possibilités d'anticipation d'attentats grâce au cyberespace et l'exploitation de signaux faibles.

Le second axe portera quant à lui sur la seconde question en intégrant notamment l'aspect séparatiste à la notion de terrorisme. Cela permettra d'étudier le concept de guerre hybride et de cyberguerre. Après cet état de l'art des nouveaux concepts, l'étude portera sur l'usage du cyberespace par des groupes terroristes et sur les États luttant contre eux dans le cadre d'opérations militaires. Les opérations dans le cyberespace étant pour les États une nouvelle arme d'emplois, des doctrines ont vu le jour ces dernières années. Ainsi, une dernière partie proposera un regard croisé entre les doctrines encadrant les actions militaires dans le cyberespace de différents pays.

1.4 État de l'art et méthode d'enquête

Le phénomène d'utilisation de l'Internet par des groupes terroristes a fait l'objet d'un certain nombre de publications, notamment depuis l'utilisation intensive des réseaux sociaux par l'État islamique pour assurer sa propagande. Néanmoins, bon nombre de ces publications s'articulent uniquement autour d'Internet et d'une utilisation à des fins de propagande. L'objectif des recherches documentaires était alors de réussir à corréler ces informations à l'abondance d'idées et de travaux menés sur le cyberespace afin d'élargir le sujet au cyberespace, et plus seulement à l'Internet et à la propagande. L'enjeu dans le cadre du mémoire réside dans la sélection des sources et leur mise en perspective, d'autant plus que les notions afférentes au cyberespace et au terrorisme ne font pas l'objet de consensus. Dans le cadre de la recherche documentaire, des difficultés ont émergé quant à l'accès à certaines informations. Ainsi, par exemple, il aurait été intéressant de mener une étude sur le contre-terrorisme dans le cyberespace. Cependant, ce domaine étant de la compétence des services de renseignement, l'accès à de telles informations s'avère impossible.

Afin d'étudier de façon plus concrète les phénomènes évoqués, une enquête portera sur l'attentat de Conflans-Sainte-Honorine le 16 octobre 2020. Celle-ci tentera de retracer les événements ayant eu lieu sur le cyberespace avant, pendant et après le passage à l'acte terroriste. Pour ce faire, l'enquête se déroulera principalement par une étude de terrain grâce aux messages et aux réactions sur les réseaux sociaux qui ont été au cœur de cet attentat et des événements l'ayant suivi. [1]

1. Tout contenu de représentation d'acte terroriste ou faisant l'apologie du terrorisme trouvé lors de l'enquête sera signalé aux autorités au travers de la plateforme PHAROS.

Chapitre 2

Occupation du cyberespace par des groupes terroristes : entre cyberterrorisme et cyberdjihadisme

L'occupation du cyberespace par des groupes terroristes renvoie inéluctablement l'idée de « cyberterrorisme ». Cependant, ce terme est encore mal défini et très théorique. Sans relever du cyberterrorisme, il est indéniable que des groupes terroristes se sont approprié le cyberespace, à l'image de l'État islamique et ses vastes opérations de propagande renvoyant alors à la notion de « cyberdjihadisme ». Cette appropriation du cyberespace par des groupes terroristes pose alors la question de l'exploitation, notamment au travers des signaux faibles, de cette présence afin de détecter tout potentiel passage à l'acte.

2.1 Le cyberterrorisme, une notion encore au stade embryonnaire

2.1.1 Le cyberterrorisme, une crainte plus qu'une réalité

Tout comme la définition du terrorisme, aucun consensus ne se dégage autour de la définition du cyberterrorisme. Il existe cependant deux grands axes de définition :[16]

- Le cyberterrorisme correspond à l'usage du cyberespace à des fins terroristes (utilisation d'outils de communication, des ressources du cyberespace à des fins de renseignement pour planifier une attaque...).
- Le cyberterrorisme se définit par les cyberattaques que peuvent mener des terroristes, que leurs conséquences soient cloisonnées sur le cyberespace (service du cyberespace tel qu'un site web rendu inaccessible) ou dans le monde physique (cyberattaque provoquant un accident industriel par exemple).

Étant donné cette absence de définition claire, la qualification d'un acte de cyberterrorisme est donc complexe. De plus, par sa nature immatérielle, l'attribution d'un acte à un auteur est bien plus complexe. L'anonymat du cyberespace rend également

impossible l'identification d'un utilisateur et donc l'attribution de ces actions. Seules d'éventuelles revendications (qui peuvent être fausses, à l'image de la cyberattaque contre TV5 monde) peuvent permettre de rattacher un acte à son auteur.

La première piste de la définition portant sur l'usage du cyberespace à des fins terroristes se heurte à divers problèmes. En effet, l'utilisation de celui-ci par des groupes terroristes à des fins de communication ou de recherche d'informations en vue de perpétrer une attaque apparait comme une utilisation normale de ce dernier ; elle se différencie uniquement par l'objectif recherché au-delà de cette utilisation, à savoir la réalisation d'un acte terroriste. Hormis des méthodes d'enquête intrusives et allant à l'encontre des libertés individuelles, il est impossible d'identifier une utilisation à caractère cyberterroriste des ressources du cyberespace. La lutte envers l'utilisation standard du cyberespace par des groupes terroristes relève davantage du domaine du renseignement, avec les problèmes qui y sont rattachés (juridiques, éthiques vis-à-vis du risque d'abus...).

En ce qui concerne la seconde piste de définition du cyberterrorisme, elle reste pour sa part relativement théorique. À l'heure actuelle aucune cyberattaque d'ampleur avec des conséquences importante à l'encontre d'infrastructures critiques n'a été recensé (site Internet important rendu indisponible, système d'information d'un Opérateur d'Importance Vitale – OIV - ou d'un de ses Points d'Importance Vitale - PIV). Néanmoins, les gouvernements et acteurs du secteur sont très conscients des risques de cyberattaques (de nature terroriste ou non) et s'adaptent en conséquence.

La question des compétences et de la complexité permet également de douter de la capacité d'une organisation terroriste de mener à bien une telle attaque. À titre d'exemple, le virus *Stuxnet*, très efficace mais uniquement sur les usines de centrifugeuses iraniennes).[17]

La question des compétences et de la complexité permet également de douter de la capacité d'une organisation terroriste de mener à bien une telle attaque. À titre d'exemple, le virus Stuxnet, réputé pour avoir retardé le programme nucléaire iranien en déréglant les centrifugeuses d'enrichissement de l'uranium, a nécessité selon les estimations plus de six mois de travail à une équipe d'une dizaine d'individus. Cette charge de travail, ajoutée aux compétences nécessaires (divers ingénieurs dont certains spécialisés dans des domaines de pointe et très précis relatifs à la cible visée) pose alors la question de la possibilité pour un groupe terroriste de mener une cyberattaque lourde de conséquence.[18]

Au vu de la complexité des opérations de cyberattaque, il semble donc que les groupes terroristes ne s'intéressent pas à cet aspect. De plus, du côté de la cybercriminalité, pourtant plus expérimentée et dédiée à ce domaine, les effets des cyberattaques sur des sites industriels ont jusqu'à présent impacté essentiellement le critère de disponibilité des services au travers de ransomware (virus bloquant un système d'information en chiffrant les données de l'utilisateur qui doit alors payer une rançon

pour récupérer les données). Ces cyberattaques n'ont pas entrainé de désorganisation extrême d'un système, voire d'un État, et encore moins entrainé des répercussions importantes dans le monde physique (dégâts matériels, morts).

La perte de disponibilité d'un système d'information pour un établissement peut néanmoins provoquer des morts. En septembre 2020, les autorités allemandes ont annoncé la mort d'une patiente des suites d'une cyberattaque. La paralysie du système informatique de l'hôpital, provoquée par un ransomware, a empêché la prise en charge de la patiente, entrainant son décès. Cet acte constitue le premier décès rattaché à une cyberattaque en Europe. Il relevait néanmoins d'un groupe de cybercriminels qui ne souhaitait pas provoquer la mort d'un patient.[19]

Cependant, la paralysie des systèmes d'informations par des ransomwares relève d'attaques très peu discriminées et diffusées à grande échelle. Les impacts sont donc en général mineurs. Le cas des hôpitaux est particulier du fait de l'urgence de l'activité. Notons tout de même que les groupes cybercriminels déclarent éviter les cyberattaques d'infrastructures de santé par acquit de conscience (bien qu'ils continuent dans la pratique). À l'heure actuelle, il n'existe aucun antécédent de ransomware visant une infrastructure hospitalière émanant de groupes terroristes dans le but de désorganiser le système et entrainer la perte de vies humaines.[20]

Les actes terroristes sont bien souvent caractérisés par la recherche de la mort d'individus, notamment de civils. L'absence de ce facteur dans le cadre d'une cyberattaque par un terroriste pourrait ainsi expliquer pourquoi nous ne sommes aujourd'hui pas confrontés à cette problématique. C'est en effet une opération longue et complexe aux impacts psychologiques relativement faibles.

Au milieu de cette nuée de définitions, des experts s'accordent à dire que le cyberterrorisme demeure une notion hypothétique. Ces derniers considèrent que les principaux risques à l'heure actuelle s'articulent davantage autour de la propagande sur Internet par des groupes radicaux. Selon Raffaello Pantucci, chercheur sur les questions liées au terrorisme, Internet permet l'autoradicalisation des individus et favorise le passage à l'acte par des individus isolés. [21] Les actes isolés sont intrinsèquement liés au terrorisme low cost au vu du peu de moyens techniques et financiers pour mener un attentat d'envergure.

La notion de cyberterrorisme peut également être abordée d'un point de vue sociologique. Celle-ci exprime en effet deux grandes craintes de la société occidentale : la peur de la technologie et la peur du terrorisme. Le terme « cyberterrorisme » permet de les englober, sans en avoir une définition précise ni d'antécédent, cependant il suffit à lui seul pour inspirer la peur.

La notion de cyberterrorisme a néanmoins son importance par le sens que lui donnent les États. En effet, à l'image des États-Unis d'Amérique, la lutte contre le terrorisme permet d'étendre le sujet jusqu'au cyberespace en justifiant qu'il est utilisé

par des individus représentant un risque pour la sécurité nationale. Cette extension permet alors de justifier les réponses des États dans le cyberespace face aux terroristes avec les dérives qui en découlent (affaire Snowden en 2013 par exemple).

Nous pouvons néanmoins considérer que le cyberterrorisme n'englobe pas l'action de groupes terroristes séparatistes. L'action de ces derniers sur le cyberespace relèverait davantage de la cyberguerre ; les cyberattaques sont en effet un moyen d'appuyer des opérations physiques (diminution des capacités de l'ennemi, désorganisation de la société afin de tirer profit du chaos engendré...).

2.1.2 Quelles formes pourrait prendre le cyberterrorisme ?

Le cyberterrorisme, dans sa notion caractérisée par une cyberattaque aux conséquences limitées au cyberespace ou non, représente des menaces qui se doivent d'être envisagées tant pour les États que pour les acteurs privés, notamment lorsque des infrastructures sont critiques, tels les OIV en France. Le cyberespace est en effet un domaine désormais à part entière et il semble par conséquent peu probable qu'il n'intéresse pas les groupes terroristes, à l'image de la criminalité qui s'est déjà très bien positionnée sur le cyberespace.

Afin de mieux comprendre les potentielles conséquences du cyberterrorisme, nous pouvons étudier diverses situations dans lesquelles une cyberattaque pourrait avoir des conséquences qui intéresseraient des groupes terroristes.

Dans un premier temps, nous pouvons reprendre l'exemple de cyberattaques visant les infrastructures hospitalières et les placer dans un contexte d'attaque terroriste. Tout comme dans le cadre d'une action cybercriminelle, des terroristes pourraient utiliser un ransomware qui chiffre les données des systèmes d'information, les rendant indisponibles afin de dégrader le fonctionnement de l'hôpital. On se retrouverait alors dans une situation similaire à celle qui a entrainé la mort d'une patiente en Allemagne. Dans des attaques plus subtiles mais qui nécessitent davantage de connaissances du système, une cyberattaque pourrait modifier les données (impact sur le critère d'intégrité), mettant alors la vie des patients en jeu (par exemple une fausse indication du groupe sanguin). Néanmoins, viser des hôpitaux n'entraînerait pas de nombreux décès (on recense actuellement un seul décès pour plusieurs milliers de cyberattaques sur des hôpitaux). Les cyberattaques d'infrastructures de santé par des terroristes semblent donc peu probables étant donné le faible intérêt qu'elles représentent pour eux. Cependant, une campagne de cyberattaques envers les hôpitaux en période de forte affluence pourrait avoir des conséquences bien plus importantes (par exemple une cyberattaque durant un plan blanc déclenché après une attaque terroriste par exemple). Un tel scénario relèverait cependant d'une attaque très minutieuse et de très grande envergure, demandant de mobiliser de nombreuses compétences (organisationnelles et techniques).

Dans un second temps, nous pouvons nous intéresser au domaine des transports, notamment aériens et maritimes. Les domaines aérien et maritime partagent la même spécificité : l'extrême dépendance à des outils de navigation, des capteurs et divers instruments afin d'assurer la sécurité. De plus, le secteur aérien est pour sa part une cible de choix, un avion étant très vulnérable et transportant plusieurs centaines de passagers.

Une étude menée en 2018 a permis d'étudier l'impact d'une cyberattaque auprès des pilotes d'avions.[22] Dans le cadre de cette étude, une simulation a été menée, dans laquelle une cyberattaque change la position d'une station radio émettrice indiquant au pilote le chemin à emprunter afin d'approcher en toute sécurité d'une piste d'aéroport. Le but d'une telle manœuvre est de désorienter un appareil et son équipage afin de le conduire à sa perte et donc à un nombre très élevé de morts. De plus, l'impact psychologique d'une telle cyberattaque serait conséquent auprès des populations et préjudiciable pour le secteur aérien, à l'image des attentats du 11 septembre 2001 (fermeture de l'espace aérien américain pendant quatre jours, diminution du trafic aérien à cause de la peur engendrée auprès des usagers). Bien que lors des simulations aucun cas d'accident fictif d'appareil n'ait été recensé, l'étude a permis de mettre en évidence le manque de formation et d'entrainement des pilotes face à une cyberattaque qui pourrait être préjudiciable et dangereuse en situation réelle. De plus, l'étude précise que l'objectif de la simulation de cyberattaque était d'avoir un effet léger et non contraignant, les conditions étaient donc favorables pour que les pilotes puissent garder l'appareil en sécurité. La cybersécurité du secteur aérien se pose également au niveau de l'appareil en lui-même depuis que les avions sont de plus en plus interconnectés et dépendants de systèmes d'information. Les instruments sont désormais essentiellement numériques (cockpit rempli d'écrans et capteurs interconnectés par un réseau) et l'ouverture de réseaux accessibles aux passagers expose l'appareil au risque d'une passerelle entre ce réseau non protégé et le réseau critique de navigation et de capteurs de l'avion. Ainsi, à titre d'exemple, la Fédération Américaine d'Aviation (FAA) a émis un avertissement concernant le Boeing 777 face à l'augmentation de la connectivité avec des réseaux externes, tels que les services de divertissement et d'informations aux passagers, qui n'existaient pas auparavant et sont sources de potentielles faiblesses pouvant être exploitées lors d'une cyberattaque.

Au niveau du secteur maritime, nous pouvons nous baser sur une étude de 2014 portant sur l'évaluation de la sécurité du système automatique d'identification (AIS).[23] Cet équipement permet aux navires de transmettre leur position et des informations entre eux, mais également de recevoir les informations des stations à terre. Ce système permet d'assurer la sécurité des navires (système anticollision, marquage des zones de danger, diffusion d'alerte...). L'étude met en lumière les différentes attaques qui peuvent être menées envers un navire ou une zone de navigation sans avoir besoin d'être à bord d'un bâtiment. L'AIS se base sur les ondes radio, il est donc possible pour un individu d'émettre de fausses informations et de leurrer les systèmes d'information des navires (création d'un faux bateau ou d'une zone de danger pour forcer un changement de cap par exemple). Une cyberattaque sur le système pourrait ainsi permettre à un attaquant de modifier la course d'un navire (d'autant plus que les pilotes automatiques des navires se basent sur les informations du système AIS) et l'amener

dans une zone de navigation dangereuse, voire en collision avec un autre navire. Les conséquences seraient alors la destruction du navire, entrainant alors potentiellement des décès parmi les passagers dans le cadre des bateaux de croisière. Un fort impact économique peut également être envisagé dans le cadre d'une destruction d'un cargo transportant de nombreuses marchandises. Se pose également la question écologique d'un tel accident, d'autant plus si un pétrolier est victime d'une telle attaque. L'étude tend à démontrer la simplicité d'une telle cyberattaque. Pour des terroristes, la complexité résidera dans la planification et l'élaboration d'un scénario permettant d'avoir des impacts lourds de conséquences en termes de vies humaines et psychologiques auprès de la population.

Enfin, dans un dernier temps, nous pouvons nous pencher sur le cas des conséquences d'une cyberattaque sur des infrastructures industrielles et notamment énergétiques. L'arrivée des systèmes d'information dans le secteur énergétique a été lente à cause des cycles d'investissement qui sont relativement longs. Ce financement sur le long terme a également des conséquences sur les systèmes d'information et leur sécurité ; ceux-ci deviennent âgés et ont été conçus lorsque la cybersécurité n'était pas un élément pris en compte, exposant alors les systèmes à des vulnérabilités. Par le passé, des cyberattaques ont provoqué la privation d'électricité auprès de la population ; ainsi, en 2015, l'Ukraine a perdu trente postes électriques de son réseau, impactant plus de 200 000 personnes pendant de nombreuses heures. La perte de disponibilité du réseau électrique désorganise la société mais ne provoque pas de dégâts matériels ou humains (les infrastructures critiques disposent en général de générateurs électriques de secours). Cependant, nous pouvons imaginer des cas de cyberattaques qui impacteraient des systèmes d'informations liés au fonctionnement d'un site de production, notamment nucléaire. L'objectif serait alors de mener à un dysfonctionnement du site entrainant un accident industriel pouvant être lourd de conséquences en termes de dégâts matériels et humains. De plus, une telle cyberattaque impacterait l'aspect psychologique auprès de la population vis-à-vis de la crainte du nucléaire. Cependant, de telles actions seraient complexes à mener et nécessiteraient d'avoir des connaissances dans le domaine, à l'image du virus Stuxnet qui a demandé une charge de travail conséquente à une équipe d'ingénieurs spécialisés dans le domaine.[24]

2.1.3 Conclusion

Actuellement, la notion de cyberterrorisme semble davantage relever d'un mythe qui retranscrit l'expression d'une crainte des États et des populations. Du fait du manque d'antécédents et de menaces concrètes à l'heure actuelle, le cyberterrorisme représente donc un potentiel domaine de risques futurs et non une réalité à laquelle doivent actuellement faire face les États. Néanmoins, les risques de réalisation d'une cyberattaque aux effets catastrophiques ne sont pas inexistants. Ces cyberattaques ne sont pour l'heure pas menées, au vu des compétences qui peuvent être requises. Cependant, nous ne pouvons pas négliger la potentielle montée en compétence de groupes terroristes dans le domaine cyber (radicalisation d'individus formés, autoformation d'individus déjà radicalisés).

2.2 L'État islamique et le cyberdjihadisme

2.2.1 L'État islamique et le cyberespace : l'apogée du cyberdjihadisme

Concrètement, le cyberdjihadisme se définit par l'utilisation des technologies du cyberespace (en particulier les réseaux sociaux sur l'Internet) permettant de mener à bien une propagande djihadiste. Cette propagande a alors divers objectifs permettant à la fois de fidéliser à la cause les membres de l'organisation mais également de recruter de nouveaux individus. Ce recrutement était indispensable au vu des ambitions de l'État islamique en termes de contrôle de territoire et d'instauration d'un État.

En 2013, l'État islamique comprend l'importance des images et de leur potentiel pour transmettre un message et se dote ainsi d'une branche médiatique et d'un studio de production de vidéo. L'organisation terroriste va même jusqu'à assurer la traduction des vidéos dans des langues occidentales, dont le français. L'approche de l'État islamique face à la production de vidéos est nouvelle ; en effet les autres groupes terroristes se contentaient de vidéos peu travaillées, non traduites et très peu diffusées. Les vidéos étaient alors principalement à destination des autorités afin de prouver la détention d'un otage et faire passer les revendication (méthode notamment employée au Liban dans les années 1980) ou de l'exécution d'un otage (méthode d'Al-Qaida).[25]

L'État islamique a alors révolutionné l'approche d'un groupe terroriste en termes de communication, dont les productions audio-visuelles et leur diffusion sur le cyberespace (sites web de propagande, réseaux sociaux).

Les productions vidéo de l'État islamique sont qualifiées de « productions hollywoodiennes » : les vidéos sont filmées en haute définition, certains plans et mouvements de caméra rappellent des plans de blockbusters américains, les vidéos sont montées et le son est retravaillé par-dessus une musique. Dans son livre *« Daech, le cinéma et la mort » [éditions Verdier, 2016]*, Jean-Louis Comolli, réalisateur français, distingue deux types de films produits par l'État islamique :[26]

— Les premiers prennent davantage le format de clips vidéo imprégnés de violence et de terreur. Ces vidéos ont pour vocation de choquer l'ennemi, de retranscrire la détermination du groupe, d'inspirer la crainte chez l'adversaire en lui montrant le sort qui lui est réservé en cas de capture. Ces vidéos courtes sont donc en général des exécutions d'otages ou de prisonniers de guerre par des moyens inhumains (noyés, brûlés vifs, écrasés par un char d'assaut, décapitation...). Au cours de ces vidéos, les messages oraux portés par les bourreaux sont avant tout vindicatifs envers l'ennemi.

— Les secondes vidéos sont quant à elles beaucoup plus travaillées et bien plus longues. Le format ressemble alors davantage à un film scénarisé faisant passer un message de propagande et d'embrigadement. Dans ces films, l'État islamique propose une succession de modèles justifiant de s'engager dans l'orga-

> nisation (rejoindre une communauté, partager une idéologie commune, fonder une famille, défendre l'islam...). Ces films, apparus un peu plus tard, sont moins axés sur la violence afin de normaliser le califat et de maintenir une illusion de légitimité sur le monde musulman, fortement détérioré par les atrocités commises envers des musulmans dans la première catégorie de films.[27]

L'utilisation de l'Internet pour diffuser du contenu djihadiste est un concept ancien, fruit du théoricien djihadiste Abu Masab al-Sûri en 2004. Ce dernier voyait dans l'utilisation de l'Internet le potentiel d'un recrutement décentralisé et une diffusion à grande échelle. Il a fallu attendre un peu moins de 10 ans pour que cette théorie soit appliquée par l'État islamique et en constater les effets en termes de recrutement et de radicalisation.

Il peut être intéressant de cerner le profil des personnes s'étant radicalisées. En 2015, sur les 3 142 personnes signalées pour radicalisation, plus de 25 % étaient mineures et ont reconnu le poids que l'Internet a joué dans leur radicalisation. [28] De manière générale, la radicalisation opère chez un public particulièrement jeune. En 2017, l'âge moyen des djihadistes majeurs condamnés par la justice française était de 24 ans. Presque la moitié des individus radicalisés n'ont pas de diplôme et plus d'un tiers est sans emploi. [29] Nous constatons donc que les profils de djihadistes sont marginalisés et souffrent d'un manque d'éducation facilitant les opérations d'endoctrinement à leur encontre grâce à des vidéos pseudo-scientifiques..

Ces jeunes sont également happés par les algorithmes des réseaux sociaux et des moteurs de recherche qui ont tendance à restreindre le champ des recherches aux contenus déjà trouvés. Les individus s'enferment donc dans une bulle informationnelle accélérant leur endoctrinement. De plus, d'un point de vue psychologique, des études cliniques tendent à démontrer que le visionnage d'images violentes, à l'instar de la première catégorie de vidéos produite par l'État islamique, appelle à visionner davantage d'images du même type dans l'objectif de comprendre l'image et de se l'approprier.[30]

Afin de trouver des réponses aux questions soulevées par les vidéos, les individus en cheminement vers la radicalisation vont généralement rejoindre des groupes de discussion sur les réseaux sociaux, voire être contactés par un recruteur qui scrute les engagements sur les publications en lien avec la mouvance radicale. À partir de là, les recruteurs vont alors mettre en avant la communauté promise par le groupe dans les vidéos en créant un lien presque affectif, fraternel, entre recruteur et recruté. Le recruteur va alors envahir l'espace émotionnel et informationnel du recruté jusqu'à son aliénation et sa soumission à la cause.[31]

Contrairement à ce que l'on pourrait penser, la stratégie de recrutement et de propagande de l'État islamique ne s'est pas contentée de séduire des hommes en vue des combats armés à mener. L'État islamique a en effet axé une grande partie de sa propagande d'endoctrinement autour des femmes. Cela était nécessaire au vu de l'ambition de construire un Califat paradisiaque où les combattants auraient des épouses.

Néanmoins, les valeurs fondamentalistes de l'État islamique envers la femme rendent complexe l'instrumentalisation de ces dernières. La charia entravant également les relations hommes/femmes, les habitudes sur le cyberespace s'en sont également retrouvées impactées ; les groupes de discussion sont en général non mixtes. Cependant, cette séparation peut également être observée d'un point de vue stratégique. En effet, avoir deux communautés séparées peut laisser penser que chacune d'entre elles est active et forte de nombreux membres. Ainsi, les futurs combattants penseront que de nombreuses épouses potentielles les attendent dans le califat, et pour les femmes qu'elle rejoindront une communauté d'entraide, heureuses de leur vie dans le Califat.

La stratégie de l'État islamique autour des femmes s'articule autour d'un certain nombre d'axes majeurs évoqués dans des publications sur les réseaux sociaux, dont Twitter qui assure plus de visibilité publique que Facebook :

— L'aspect communautaire poussant à l'entraide les femmes ayant effectué *l'hijrah* (action d'immigrer vers une terre sainte où est appliquée la charia).

— La vie déresponsabilisante promise au travers d'un système d'assistanat (nourriture et logement gratuits).

— La promesse d'une vie sans oppression vis-à-vis de la pratique de l'islam.

— La promesse d'un destin exceptionnel en participant à la mise en place de l'État islamique et en s'assurant l'accès au paradis après la mort.

— La puissance que la femme aura sur son foyer, à l'image d'une lionne (image souvent utilisée par la propagande).

Les messages publiés par des femmes prétendument présentes dans le Califat permettent aux prétendantes d'avoir un premier contact et de bénéficier d'une aide pour rejoindre les territoires du califat. Des guides ont même été rédigés afin de préparer au mieux le départ des femmes, soulignant l'importance de la présence de femmes dans le califat aux yeux de l'État islamique.[32]

Enfin, le cyberdjihadisme instauré par l'État islamique a également permis de diffuser des messages appelant à la réalisation d'actes terroristes en Occident. Ainsi, en 2015, dans un reportage tourné par un reporter britannique otage du groupe puis diffusé sur l'Internet, un combattant francophone interrogé appelle les musulmans français à commettre des attentats ;[33]

> *« Partez en opération seul, soyez un loup solitaire, à vous tout seul vous pouvez être une armée. (...) J'encourage tous mes frères qui sont en France à défendre votre religion. Tuez-les avec des couteaux, au minimum crachez-leur à la figure. (...) Les musulmans en Occident, vous êtes des milliers, vous pouvez faire des carnages. »*

L'État islamique a également joué du sensationnalisme créé par leur propagande sur l'Internet en sachant que celle-ci allait être citée par les médias classiques en Occident et donc diffusée à grande échelle. Ainsi, pour reprendre l'exemple précédent, le

message qui était à la base cantonné au cyberespace et principalement visionné par des sympathisants à la cause radicale a été véhiculé massivement par la presse auprès de toute la population.

L'État islamique a ainsi fait passer le djihadisme traditionnel à l'ère du numérique, tant sur le plan du recrutement de combattants, de la construction du califat avec l'endoctrinement de femmes et de la propagande incitant les musulmans occidentaux à commettre des attentats. En ce sens, l'État islamique a connu une apogée en termes d'occupation du cyberespace que l'on peut qualifier de cyberdjihadisme et qui a pris de court de nombreux États et acteurs de l'Internet.

2.2.2 La France face au cyberdjihadisme : entre prévention et tâtonnement juridique

Fin 2014, le procureur de la République de Paris, François Molins, estime qu'il y avait plus de 1 100 Français impliqués dans des filières jihadistes, dont 376 présents dans des zones de combats. François Molins indique également qu'une grande partie de cette population est jeune (entre 18 et 22 ans) et s'est convertie (à hauteur de 20 %). Face à ce constat alarmant, le gouvernement décide de contre-attaquer début 2015 en lançant un site officiel contre le cyberdjihadisme, *stop-djihadisme.gouv.fr*. Bernard Cazeneuve, alors ministre de l'Intérieur, déclare que ce site a pour vocation de *« démystifier des démarches d'endoctrinement sectaire »*. À son lancement, le site affichait en première page une vidéo intitulée « Ils te disent... ». Cette dernière reprenait les codes de propagande de l'État islamique sur fond d'images chocs extraites des films de propagande de l'organisation.[34]

L'analyse de cette vidéo [35] est intéressante à mener afin de comprendre ses répercussions et son accueil. Cette vidéo d'à peine deux minutes commence par montrer l'approche d'un individu sur Facebook par un recruteur de l'État islamique à la suite de son activité et de ses engagements sur des publications djihadistes. S'ensuit alors la démystification d'axes majeurs de la propagande de l'État islamique. Chaque axe de recrutement apparait en texte, précédé de la mention « Ils te disent : » sur des images qui se veulent positives pour le groupe (manifestations festives, moments de paix). Puis une phrase déconstruisant la propagande apparait sur des images de crimes et/ou d'horreur en noir et blanc précédées de la mention « En réalité ». Ce procédé est répété 4 fois :

— « Ils te disent : Sacrifie-toi à nos côtés, tu défendras une juste cause » ; « En réalité, tu élèveras tes enfants dans la guerre et la terreur ». Les images de crimes sont alors un groupement de diverses séquences d'exécutions perpétrées par l'État islamique. Cet axe vise à dissuader les potentiels futurs combattants.

— « Ils te disent : viens fonder une famille avec un de nos héros », « En réalité, tu découvriras l'enfer sur terre et mourras seul, loin de chez toi. ». Les images de fond reprennent des séquences tournés auprès de famille réfugié avec des enfants en pleures. Ce sont ici les femmes qui sont ciblé afin de les inviter à ne

pas rejoindre le califat.

— « Ils te disent : rejoins-nous et viens aider les enfants syriens » ; « En réalité, tu seras complice du massacre de civils ». Les images de fond sont de nouveaux celles d'enfants réfugiés en pleurs. Le message tente ici de décrédibiliser la légitimité de l'État islamique.

— « Ils te disent : tu vis dans un monde de mécréants impurs, la vérité est ici » ; « En réalité, comme seules vérités tu découvriras l'horreur et la tromperie ». Les images de fond sont celle d'hommes et de femmes morts, exhibés en étant crucifiés ou trainés derrière un véhicule. L'objectif est de décrédibiliser une nouvelle fois la légitimité de l'organisation et de ses prétendues bonnes actions pour le monde musulman.

Le vidéo reprend donc les principaux axes de propagande qui ont été mentionnés précédemment et tente de les déconstruire. Cependant, bien que le message écrit soit indéniable et fondé, la réalisation audio-visuelle est discutable. En effet, comme cela a été évoqué précédemment, une partie des candidats au djihad cherchent des images d'exactions et de violence et y sont pour certains habitués, l'effet choc est donc estompé. D'autant plus, l'impact d'une telle vidéo auprès du public susceptible de se radicaliser est incertain au vu du rejet des informations de l'État et de leur isolement dans une bulle informationnelle de propagande djihadiste.

Fin 2016, selon les autorités, cette campagne et la campagne suivante (« Toujours le choix », une sorte de jeu interactif où le joueur incarne un jeune qui doit ne pas se laisser embrigader en effectuant divers choix) ont été un succès au vu de la baisse du nombre de départs. Il est cependant impossible de dire si les campagnes de prévention en sont réellement la cause et s'il ne s'agit pas là d'une corrélation. Aujourd'hui, la vidéo n'est plus accessible sur le site, peut-être un aveu d'une réalisation audio-visuelle maladroite. Cependant, le jeu interactif, plus conventionnel, est toujours accessible sur le site.

La France ne s'est pas contentée d'un arsenal préventif que l'on pourrait qualifier de contre-propagande au sein d'une guerre de l'information afin de lutter contre le cyberdjihadisme. Ainsi, en novembre 2014, à la suite d'une procédure accélérée engagée, le gouvernement a voté une loi permettant de renforcer *« les dispositions relatives à la lutte contre le terrorisme »*. L'article 5 de cette loi insère l'article 421-2-5 au code pénal afin de lutter contre la propagande et l'apologie du terrorisme. Selon les dispositions de cet article, le fait *« de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement »*. Cependant, la peine peut être portée à sept ans d'emprisonnement *« lorsque les faits ont été commis en utilisant un service de communication au public en ligne »*. [36] La loi s'est donc adaptée face à l'émergence du cyberdjihadisme. Cependant, en termes d'application, les enquêtes judiciaires se sont bien souvent retrouvées confrontées à la barrière de l'anonymat de l'Internet empêchant d'identifier clairement les auteurs de contenus de cyberdjihadisme.

En 2016, une loi est adoptée par le gouvernement afin de *« renforcer la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale »*. L'article 18 crée ainsi l'article 421-2-5-2 du code pénal qui permet de sanctionner *« le fait de consulter habituellement un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes »*. Cette loi permet donc d'aller plus loin dans la lutte contre le cyberdjihadisme en élargissant les sanctions pénales aux potentiels candidats djihadistes et non plus seulement aux créateurs de contenus.[37]

Cependant, à la suite d'une question prioritaire de constitutionnalité (QPC) la loi a été abrogée début 2017. Le conseil constitutionnel a en effet jugé que cette loi portait atteinte à la liberté de communication et que *« les autorités administratives et judiciaires disposent, indépendamment de l'article contesté, de nombreuses prérogatives, non seulement pour contrôler les services de communication au public en ligne provoquant au terrorisme ou en faisant l'apologie et réprimer leurs auteurs, mais aussi pour surveiller une personne consultant ces services et pour l'interpeller et la sanctionner lorsque cette consultation s'accompagne d'un comportement révélant une intention terroriste, avant même que ce projet soit entré dans sa phase d'exécution. »*. La simple consultation de sites djihadistes ne fait plus d'un individu un suspect et potentiel terroriste pénalement responsable, cette décision QPC rappelle ainsi en quelque sorte le travail qui est nécessaire du côté des services de renseignement avant d'aboutir à une condamnation pour terrorisme.[38]

Une nouvelle loi relative à la sécurité publique, début 2017, tente de réhabiliter l'article 421-2-5-2 du code pénal en précisant que la consultation doit être accompagnée *« d'une manifestation de l'adhésion à l'idéologie exprimée »*. Sont également ajouté des motifs légitime de consultations, notamment dans le cadre de travaux journalistique ou universitaire (pour plus de précision voir annexe B - Evolution de l'article 421-2-5-2 du code pénal). Cet article est alors de nouveau sujet à une QPC quelques mois plus tard et se retrouve de nouveau abrogé, le conseil constitutionnel estimant que l'article en question *« porte une atteinte à l'exercice de la liberté de communication qui n'est pas nécessaire, adaptée et proportionnée »*.[39]

Par conséquent, en France à l'heure actuelle, seuls les auteurs d'actions pouvant être qualifiées de cyberdjihadisme sont pénalement responsables. Pénalement parlant, les individus en voie de radicalisation sont couverts tant qu'il n'y a pas d'intention matérielle de passage à l'acte. Cela explique notamment l'idée d'une relative impuissance des services de police et de renseignement face au terrorisme lorsque se produit un attentat. Ces derniers peuvent en effet avoir connaissance des individus radicalisés mais doivent avoir des éléments matériels justifiant un passage à l'acte, ce qui s'avère complexe, voire impossible, dans le cadre du terrorisme low cost qui est en général spontané et peu préparé, ce qui le rend fortement imprévisible. De plus, se pose également le problème des moyens à disposition des services de police et de renseignement pour mener des enquêtes longues et coûteuses en termes de ressources humaines sur

les individus radicalisés afin de pouvoir intercepter toute intention de réalisation d'un attentat.

2.2.3 Conclusion

En 2014, l'État islamique a connu une apogée militaire sur le terrain mais aussi dans le cyberespace au travers de vastes campagnes de propagande afin d'élargir ses rangs et d'imposer la terreur chez les ennemis. Cette médiatisation du terrorisme et de la terreur a été inédite par la forme et les moyens impliqués par l'organisation. Face à cette menace, la France est entrée dans une guerre de l'information contre l'État islamique afin d'enrayer son processus de recrutement. La France s'est également équipée d'un attirail juridique pour faire face au cyberdjihadisme en se heurtant néanmoins à plusieurs reprises à ses valeurs constitutionnelles.

2.3 Est-il possible d'anticiper le terrorisme islamiste grâce au cyberespace ?

2.3.1 Les signaux faibles de l'occupation du cyberespace par l'État islamique

L'État islamique ayant une grande présence sur les réseaux sociaux, il peut sembler intéressant de surveiller ces derniers, tant pour lutter contre la propagande djihadiste que pour repérer tout individu radicalisé s'apprêtant à passer à l'acte, mais aussi en voie de se radicaliser car il représentera une menace potentielle à l'avenir. Cette recherche de terroristes potentiels relève alors du monde du renseignement, qui peut notamment s'appuyer sur des signaux faibles.

Le concept des signaux faibles apparait en 1975 dans les travaux d'Igor Ansoff, mathématicien et économiste, qui décrit la détection des signaux faibles comme un outil permettant d'anticiper toute surprise stratégique menaçant l'organisation. Quelques années plus tard, des travaux précisent alors qu'un signal faible se définit comme *« un fait à propos duquel seules des informations partielles sont disponibles alors qu'une réaction doit être entamée, si l'on veut qu'elle soit parachevée avant impact sur la firme de l'événement nouveau » [Igor Anso, Edward J. McDonnell]*.[40]

Les signaux faibles peuvent autant s'exprimer dans le monde physique (conversion religieuse, achat d'armes, départ dans des terres de djihad, changement de comportement) que dans le cyberespace (consultation de contenus de propagande, de tutoriels pour fabriquer une bombe, activité sur les réseaux sociaux). Le développement des technologies liées aux big-datas (capacité de collecter et d'analyser un grand nombre de données numériques) ainsi que l'amélioration des algorithmes d'aide à la décision a permis de donner une seconde jeunesse au concept de signaux faibles. L'évolution de ces technologies permet ainsi aux services de renseignement engagés dans la lutte contre le terrorisme d'élargir leur champ de détection en allant chercher des individus

radicalisés ou en voie de passer à l'acte sur le terrain du cyberespace.

À partir de la littérature existante sur le sujet et en observant les similitudes entre des publications de propagande de l'État islamique, il est possible de dégager certains signaux faibles relatifs à la présence de l'État islamique sur les réseaux sociaux. Cependant, il est important de distinguer deux phases dans cette occupation :

— De 2014 à 2017 : la présence était directe, totalement assumée. Les messages sont explicites, sans ambiguïté, il semble donc impertinent de parler de signaux faibles dans ces cas-là, mais plutôt de signaux que l'on qualifiera de forts.

— À partir de 2018 : après des mesures visant à lutter contre la propagande sur les réseaux sociaux, les publications ont muté vers plus de discrétion et de subtilité. En ce sens, il est possible de parler de signaux faibles. Les publications passent en effet inaperçues au milieu de la masse des autres publications des réseaux sociaux mais véhiculent tout de même des messages de propagande et peuvent éventuellement indiquer un passage à l'acte chez un individu.

Entre 2014 et 2017, les signaux forts s'exprimaient avant tout au travers de l'utilisation des images, notamment par l'utilisation des photos de profils et/ou de couverture. De nombreux comptes utilisaient des photos de profils dépersonnalisés, utilisant alors le drapeau de l'État islamique ou des figures du terrorisme islamiste telles que Ben Laden. Les photos de couverture étaient quant à elles bien souvent des photos du groupes terroriste avec un drapeau ou les armes à la main.[41]

La communauté cyberdjihadiste était ensuite relativement interconnectée. Ces comptes utilisaient des hashtags communs entre eux, se suivaient et interagissaient entre eux. Néanmoins, bon nombre de comptes peuvent être en réalité des robots chargés de poster des messages prédéfinis et/ou de relayer les messages d'autre compte.[42] En 2014, l'État islamique a également conçu une application, *Dawn of Good Tidings*, qui était reliée au compte de l'utilisateur. Une fois reliée, l'application tweetait automatiquement des tweets de propagande depuis les comptes tout en variant suffisamment le contenu et la fréquence d'émission afin de ne pas se faire détecter par les filtres anti-spam du réseau social.[43]

Enfin, les publications s'articulaient autour d'un champ lexical très clair, parlant des combats en Syrie dans une langue occidentale puis utilisant des mots arabes pour parler des préceptes forts dans l'islam qui seraient alors défendus dans cette guerre (*Jennah* pour parler du paradis,*hijrah* pour parler du départ en terre de djihad, *Allah* pour parler de dieu, ...). Toujours d'un point de vue sémantique, dans les publications en français, il n'était jamais fait référence à l'écriture occidentale *Mahomet* mais à l'écriture *Muhammad* ou directement écrit en arabe.

Cependant, depuis 2018 la propagande a muté vers plus de discrétion et de subtilité afin de passer outre les contrôles automatiques et manuels des plateformes qui ont été mis en place après cette utilisation massive et non réprimée des réseaux sociaux

par l'État islamique.[44]

Tout d'abord, des signaux faibles semblent ressortir d'une certaine forme d'approbation des actions terroristes sur les réseaux sociaux par l'utilisation des emojis. Facebook permet en effet de réagir à une publication avec plusieurs emojis (pouce, cœur, visage triste, visage désapprobateur/énervé, visage en train de rire). En effet, sur certaines publications d'articles de presse mentionnant des attentats des individus, qui ne sont pas des comptes de propagande, ce qui pourrait être interprété comme un signe d'approbation et par conséquent un potentiel candidat pouvant être approché par des recruteurs qui scrutent ce genre de publications. Ce potentiel signal faible est d'autant plus renforcé quand certains des individus réagissant ainsi ont une activité sur le réseau social qui concorde avec d'autres signaux faibles.

Les messages sont désormais plus subtils, se basant sur des références symboliques. Ainsi, lors de la date anniversaire des attentats du 13 novembre 2015, des publications reprennent le refrain d'un chant djihadiste indiquant que *« c'est Valls qu'il faut remercier » [chant de L'Etat islamique, « Ma vengeance »]*. En plus des références, les messages peuvent être dissimulés dans des tournures de phrases ironiques et/ou sarcastiques, voire de réalisations visuelles (image/vidéo) détournées permettant ainsi de faire passer les messages de violence et d'apologie pour de l'humour noir.[45]

Alors qu'il existait avant un important réseau de comptes clairement définis et visibles de propagande, ces derniers ont réduit leur taille et leur fréquence de publication afin de mieux se fondre dans la masse. La présence de l'État islamique c'est donc muée vers une occupation discrète des réseaux sociaux. Contrairement aux années 2014 à 2017, détecter une publication de propagande ou d'apologie au terrorisme est plus subtil et demande davantage d'intelligence pour les repérer puis pour les interpréter au milieu de la masse d'activités usuelles sur les réseaux. Cela fait alors ressurgir l'exploitation des signaux faibles pour mieux repérer ces activités afin de lutter contre le cyberdjihadisme et repérer tout individu sous-entendant la réalisation imminente d'un attentat. Cependant, l'exploitation de signaux faibles présente un certain nombre de limites...

2.3.2 Les limites de l'exploitation des signaux faibles

Un signal faible peut être source de nombreux faux positifs (mots en arabe dans une publication tout à fait normale, utilisation d'images de l'État islamique dans une publication de presse ou similaire...). Ainsi, chaque alerte se doit d'être manuellement vérifiée, puis éventuellement d'instruire l'affaire afin d'en déterminer l'auteur et de l'amener s'il y a lieu (et que cela est possible) devant la justice. L'exploitation de l'intégralité des alertes de signaux faibles semble donc fortement limitée par les ressources humaines et/ou techniques d'une organisation. La probabilité de publications de propagande ou laissant présager d'un attentat est donc très élevée et le rapport bénéfice/coût en termes d'investissement dans de telles technologies peut se poser.

Il semble important de souligner que le traitement de ces alertes issues des signaux faibles est limité, entre autres, par les possibilités juridiques. Dans la majorité des cas, les auteurs d'attentats sont très souvent connus des services de renseignement grâce au recueil de signaux faibles (que ce soit sur le cyberespace ou dans le monde physique) en amont de leurs actes. Ils sont même pour beaucoup « fichés S ». Cette fiche S n'est en réalité qu'une inscription dans une base de données du gouvernement pour les personnes représentant une menace pour la sûreté de l'État. Ces fiches sont utilisées pour procéder à la surveillance et au traçage des individus pouvant menacer la sûreté de l'État mais elle ne permet pas à elle seule d'entreprendre une coercition envers l'individu.[46] En effet, si les signaux faibles, aussi nombreux soient-ils, constituent une indication sur un individu potentiellement dangereux, ils ne constituent pas des preuves. Des signaux faibles pouvant être émis par des individus ne représentant aucune menace pour l'ordre public.

La question de la pertinence de l'exploitation des signaux faibles peut également se traiter en regardant certains projets publics sur la question. Par exemple, en partant du constat que le vocabulaire et l'analyse sémantique des publications pouvait permettre de détecter des publications à caractère djihadiste, l'Union Européenne a lancé le projet SAFFRON. S'étalant sur deux ans entre 2016 et 2018, l'objectif était de fournir un outil en mesure de détecter les signaux faibles liés au recrutement par des groupes terroristes. Ce projet, financé à plus de 670 000€ par le fond de sécurité intérieur de l'Union européenne a cependant émis très peu de retour en termes de résultats, du moins de façon publique.[47]

Le concept d'exploitation des signaux faibles peut également être critiqué sur son fondement. Le principe est d'élaborer puis de chercher des indicateurs dans un ensemble (ici le cyberespace) permettant d'identifier un phénomène (ici du cyberdjihadisme et/ou les signes d'un passage à l'acte). Cependant, à force de trop chercher un signal dans la masse, la surinterprétation et la surréaction sont des risques bel et bien présents. Une trop forte remontée d'alertes et d'investigations à mener viennent alors corroborer les constats précédents vis-à-vis de la surcharge de travail pour les services de renseignement et de justice.[48]

En 2016, le commissaire Jean-Marc Rebouillat, chef de la Sûreté départementale du Rhône, dénonçait cette concentration sur les signaux faibles qui poussait à voir ce qui n'existait pas forcément à force de chercher. Ainsi, selon lui *« [ses services traitent] tous les événements sans rien laisser passer, le travail policier doit désormais ratisser tous les signaux, ce qui peut donner l'impression de surréagir sur des faits qui, avant les attentats, auraient pu paraître banals au quotidien. » [Propos rapporté par Richard Schittly dans un article dans Le Monde]*.[49] Cela tend donc à démontrer un potentiel effet contre-productif dans l'exploitation des signaux faibles, du moins en ce qui concerne le renseignement et le contre-terrorisme.

Enfin, l'exploitation des signaux faibles peut aller à l'encontre de l'État de droit qui prédomine en France. En effet, si les signaux faibles sont trop larges et que tout un chacun peut se retrouver fiché « S » et donc placé sous surveillance, cela peut mener à des abus. Cela peut s'illustrer grâce aux différents programmes de surveillance électronique révélés par Edward Snowden, ex-analyse de la NSA. Ces programmes américains visaient à collecter et traiter le renseignements collectés dans le cyberespace. L'orientation des surveillances était permise, entre autres, par l'exploitation de signaux faibles. Cependant, de par une définition sûrement trop large de ces signaux faibles implémentée au sein de ce programme, énormément de personnes étaient considérées comme potentiellement dangereuses et donc placées elles aussi sous surveillance ; plus de 117 000 personnes étaient suspectées lors des révélations d'Edward Snowden en 2013.[50]

L'exploitation des signaux faibles, au-delà des contraintes techniques et opérationnelles, soulève donc un point important en termes d'éthique et de respect des libertés individuelles. Les États justifient en général ces entorses aux libertés au travers du prisme de la sécurité et du contre-terrorisme. Cependant, les contestations sont nombreuses au sein de la population, qui ne semble pas forcément prête à sacrifier sa liberté pour plus de sécurité (qui est en somme relative au vu de l'opacité concernant les actions de contre-terrorisme). Pour l'heure, il semble compliqué d'estimer que l'exploitation des signaux faibles soit une bonne piste pour lutter contre le cyberdjihadisme ou repérer un passage à l'acte, que ce soit en termes de respect des libertés, de pertinence des alertes pour ne pas surcharger les services, et de moyens techniques et humains pour enquêter sur les alertes et pouvoir intervenir, notamment au travers de la justice.

2.3.3 Étude de cas : l'attentat de Conflans-Sainte-Honorine

Au travers de cette étude de cas relativement récente, l'objectif sera d'identifier les actions ayant pris place sur le cyberespace avant, pendant et après l'attentat. Pour rappel, l'attentat de Conflans-Sainte-Honorine, le 16 octobre 2020, correspond à l'assassinat par un terroriste islamiste de Samuel Paty, professeur d'histoire-géographie dans un collège. L'assassinat de cet enseignant fait suite à un cours donné le 6 octobre sur la liberté d'expression, durant lequel il a illustré son propos au travers de carricatures de Mahomet publiées dans le journal satirique Charlie Hebdo.

À la suite de ce cours, un parent d'élève va alors faire une vidéo réquisitoire envers l'enseignant, en déformant la teneur du cours de l'enseignant, visant à le faire passer pour un islamophobe. Le parent d'élève demande également l'adresse de l'enseignant (Figure 2.1). La vidéo a ensuite été partagée sur les réseaux sociaux, notamment par la Grande Mosquée de Pantin qui dispose d'une large audience (Figure 2.2).

Figure 2.1 : Publication Facebook du parent d'élève à l'origine du déferlement de haine envers l'enseignant.

Figure 2.2 : Publication sur la page Facebook de la Grande Mosquée de Pantin.
Notes : La publication était acompagné de la vidéo du parent d'éleve.

Gérald Darmanin, ministre de l'Intérieur, évoquera plus tard à propos des auteurs des publications sur les réseaux sociaux qu' *« ils ont manifestement lancé une fatwa contre ce professeur » [Gérald Darmanin en interview sur Europe 1 le 19 octobre 2020]* (une fatwa correspond à un avis juridique en islam, par abus de langage ce terme est souvent utilisé pour appeler à un meurtre au nom de l'islam). En effet, la viralité des vidéos a suscité un déferlement de haine envers l'enseignant sur les réseaux sociaux peu avant l'attentat, d'autant plus que les informations personnelles de l'enseignant (nom, prénom, adresse, lieu de travail) ont été divulguées. En ce sens, les réseaux sociaux sont à l'origine de cet attentat en permettant à des individus proches d'une mouvance islamiste ou salafiste de désigner une cible et de partager les informations nécessaires pour l'atteindre.

Peu de temps après avoir assassiné l'enseignant, l'auteur a publié un tweet, accompagné d'une photo de la décapitation, sur son compte pour revendiquer son attentat et les motivations islamiste derrière celui-ci (Figure 2.3). Avant la suppression du tweet, des réponses ont tourné l'attentat en dérision, jouant avec l'humour (Figure 2.4). Cela semble donc corroborer l'étude sur les nouveaux signaux faibles de la présence islamiste sur les réseaux sociaux en termes d'ironisation de la situation.

Figure 2.3 : Publication twitter de l'auteur de l'attentat.
Notes : La photo de la décapitation accompagnant le tweet n'apparait pas.

Figure 2.4 : Tweet en réponse au tweet en Figure 2.3 (gauche) et image de propagande diffusé après l'attentat (droite).

Après l'attentat, les publications sur Facebook de la presse à ce sujet ont eu un certain nombre de réactions avec des émojis rigolant de la situation, ce qui rejoint une fois de plus le constat précédent. Une vague de spams de messages haineux sur un fond d'islamisme a également eu lieu dans les commentaires de ces mêmes publications (Figure 2.5). Ici, le cyberespace a permis d'accentuer l'horreur de cet attentat en véhiculant des messages de haine et pouvant inciter la peur sur les réseaux sociaux. Cela peut être relié à du cyberdjihadisme. Des cyberattaques ont également eu lieu envers des sites français afin de changer leurs pages d'accueil et de vanter l'attentat. [51] Ces cyberattaques ont cependant peu impacté les systèmes, n'étaient pas revendiquées et servaient essentiellement à appuyer la campagne de diffusion de messages de haine à l'encontre de la France. De plus, elles ont dans l'ensemble mobilisé peu de compétences techniques car elles étaient le fruit de scripts prêt à l'emploi qui peuvent s'acheter sur Internet (*script kiddies*).

Figure 2.5 : Exemples de commentaires sous une publication de TF1 parlant de l'attentat.

Le compte twitter du terroriste a rapidement été bloqué. Cependant, au travers des éléments relevés il apparait que son propriétaire vivait dans un islam très pieux que l'on pourrait qualifier de salafiste. Il indiquait notamment sur son profil ne pas vouloir parler aux femmes, l'intégralité de son contenu était axé autour de l'islam (Figure 2.6) et sa photo de profil allais en ce sens (Figure 2.7). Bien que les inscriptions en russe ou en arabe ne fassent aucunement référence à un groupe terroriste ou au djihad, le code visuel utilisé (inscription en arabe sur fond noir en guise de photo de profil) peut rappeler les codes d'images à caractère djihadiste.

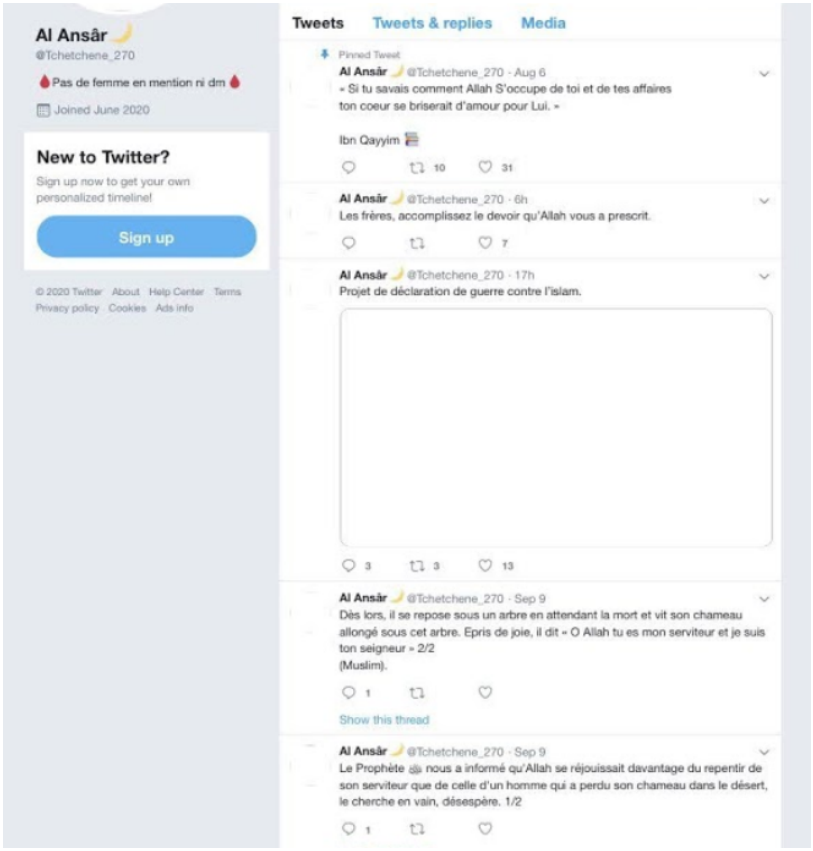


Figure 2.6 : Aperçu du compte twitter de l'auteur de l'attentat.

Figure 2.7 : Photo de profil twitter de l'auteur de l'attentat.

Bien qu'ayant de nombreux signaux faibles évoquant un individu a minima salafiste, il était impossible d'identifier un passage à l'acte à partir de ces faits ni de procéder à une interpellation ou une enquête approfondie ; c'est en effet un type de compte assez commun sur les réseaux.

Le cyberespace a été très présent au sein de cet attentat ; désignation et informations relatives à la cible, revendication et usage d'images pour propager la terreur de l'acte, amplification de l'attentat par les cyberattaques sur des sites internet ainsi que des campagnes de spam de commentaires sur des publications de presse sur Facebook.

Enfin, il peut être intéressant de se demander si la médiatisation, notamment au travers du cyberespace, de cet attentat n'a pas été à l'origine de la vague d'attentats par mimétisme qui a suivi les jours suivants ; église à Nice où 3 victimes ont été décapitées, agression au couteau d'un agent de sécurité devant le consulat français à Djeddah (Arabie Saoudite), bombe lors de la commémoration du 11 novembre au cimetière de Djeddah, sans compter les potentielles tentatives avortées à Lyon et Paris qui se sont soldées par l'arrestation d'individus possédant des couteaux.

2.3.4 Conclusion

L'exploitation de signaux faibles sur le cyberespace pour lutter contre le cyberdjihadisme ou repérer un individu s'apprêtant à passer à l'acte souffre de plusieurs problèmes. Les moyens techniques et humains employés sont conséquents, les suites judiciaires s'avèrent complexes et enfin de telles méthodes peuvent soulever des problématiques en termes d'éthique dans le renseignement (définition des signaux faibles, vie privée).

Cependant, il est important pour les États de pouvoir identifier les menaces émanant du cyberespace, comme a pu le démontrer l'attentat de Conflans-Sainte-Honorine qui est né de l'utilisation du cyberespace par des individus proches d'une mouvance salafiste, voire islamiste.

2.4 Conclusion

Rappel de la problématique : Quelles sont les formes actuelles de l'occupation du cyberespace par des groupes terroristes ?

Aujourd'hui, les groupes terroristes ne semblent pas en mesure de mener des cyberattaques pouvant perturber le fonctionnement d'une entité et/ou causer des pertes humaines. En ce sens, il semble donc trop tôt pour parler de cyberterrorisme. Cependant, à l'image de l'État islamique, des groupes terroristes ont su intégrer le cyberespace à leur champ d'action, notamment en termes de propagande. Nous avons ainsi vu naître le cyberdjihadisme, en particulier sur les réseaux sociaux. Ces mêmes réseaux sociaux peuvent fournir des informations aux services de renseignement luttant contre le terrorisme grâce à l'exploitation de signaux faibles, bien que cette exploitation ne soit pas sans limite en termes de ressources, d'utilisation sur le plan juridique et d'éthique. Le cyberespace marque également bien la porosité entre les mouvances salafistes et islamistes en termes de communication et d'idéologie. Cette porosité et l'échange d'informations qui en découle peut mener à des ciblages à des fins terroristes.

En reprenant le modèle de couches du cyberespace, nous pouvons ainsi émettre les constats suivants :

— Vis-à-vis de la couche physique et logique, les groupes terroristes sont essentiellement de simples utilisateurs et ne sont pour l'heure pas en mesure de porter atteinte aux critères DIC de ces dernières.

— En ce qui concerne la couche psycho-cognitive, celle-ci a été relativement bien exploitée, notamment par l'État islamique, au travers du cyberdjihadisme (recrutement, revendication, propagande...).

En conclusion, les groupes terroristes sont pour l'heure davantage des utilisateurs du cyberespace pour communiquer à propos de leurs actions qu'une menace. Cependant, le cyberespace constitue malgré tout un environnement favorable à une action de cyberterrorisme ayant des impacts lourds sur une entité et/ou des vies humaines.

Chapitre 3

Guerre contre le terrorisme et le séparatisme : une guerre hybride intégrant le cyberespace comme domaine de lutte

Que ce soit envers des groupes terroristes islamistes ou séparatistes, les États doivent faire face à une mutation de la guerre avec l'avènement du cyberespace et des technologies associées. Cette mutation de la guerre a donné naissance au terme de « guerre hybride », dans lequel se retrouve le concept de cyberguerre. Le cyberespace permet ainsi d'ouvrir un nouveau domaine opérationnel dans la lutte contre les groupes terroristes et séparatistes. Face à de tels changements et à l'émergence du domaine cyber dans les armées (par *cyber* nous entendrons ici l'essor des technologies numériques telles que les ordinateurs, les réseaux, les algorithmes et/ou les outils tournant sur ces systèmes), les États se sont adaptés au travers de doctrines et de plans stratégiques.

3.1 Guerre hybride et cyberguerre : quelle réalité ?

3.1.1 La guerre hybride, un concept encore flou

Le concept de guerre hybride apparait pour la première fois en 2005 dans un article rédigé par deux officiers du corps des Marines américains.[52] Les auteurs craignent notamment la prolifération d'armes, notamment NRBC, au sein de forces irrégulières. Cette prolifération est un risque envisagé au vu de l'instabilité de certains États et le risque que ces derniers s'effondrent, disséminant alors leurs stocks d'armes. Les auteurs craignent également l'émergence de groupes terroristes, potentiellement soutenus par des puissances étrangères ennemies, menant des attaques à l'encontre d'infrastructures critiques sur le territoire national. Enfin, les auteurs mentionnent le risque d'attaques envers des cibles du secteur financier mais aussi envers des systèmes numériques, incluant alors la dimension cyber qui manquait à la guerre.

La guerre hybride tient sa définition du fait que de nombreuses guerres, dont la guerre d'Irak dans laquelle les Américains étaient empêtrés au moment de la rédaction de l'article, ne peuvent être définies comme purement régulières ou irrégulières.

— La guerre régulière respecte un code, le droit de la guerre (aspect juridique). Les belligérants sont identifiables par leur tenue commune et l'engagement politique des acteurs (aspect politique). La guerre régulière est également définie par son aspect stratégique qui consiste dans sa finalité à neutraliser et prendre le dessus sur l'adversaire et d'avoir le contrôle du terrain.

— La guerre irrégulière fait quant à elle référence à une guerre où plusieurs cas de figure peuvent se rencontrer et se traduit bien souvent par des actions de guérilla, l'existence d'une guerre asymétrique et/ou d'actes de terrorisme, certains parleront même de guerre de harcèlement. L'irrégularité est bien souvent marquée par l'absence de distinction entre les combattants et les non-combattants. L'ennemi est alors dissimulé parmi la population qui ne le dénoncera pas, soit par peur des représailles soit par soutien. Globalement, si un des aspects de la guerre régulière est enfreint (juridique, politique, stratégique) la guerre sera jugée irrégulière.[53]

Cependant, la non-conformité à un des aspects n'implique pas forcément une irrégularité totale de la guerre et la réalité des opérations ne peut s'en tenir à un modèle binaire. De ce constat et des nouvelles menaces est né le concept de guerre hybride, qui se veut être un entre deux pour mieux définir la réalité des futurs conflits armés.

L'OTAN définit la guerre hybride comme l'entrecroisement de la guerre conventionnelle et non conventionnelle, régulière et irrégulière, tout en prenant en compte l'aspect cyber et informationnel de la guerre. Néanmoins, les États membres ne parviennent pas à un consensus sur la définition exacte et précise de la guerre hybride au vu des menaces protéiformes que ce concept renferme. En effet, les pistes de définitions précédemment évoquées laissent sous-entendre que toute guerre est hybride, la guerre étant bien souvent un entrecroisement des notions de régularité et d'irrégularité. Or, le concept de guerre hybride est d'englober un nouveau type de conflit. Ainsi, sans définition unanime, la guerre hybride est bien souvent illustrée au travers d'exemples.

L'exemple du conflit israélo-libanais de 2006

Un des premiers exemples de guerre hybride se retrouve dans le conflit israélo-libanais de 2006. Dans ce conflit opposant l'armée israélienne au Hezbollah (parti politique et groupe islamiste basé au Liban), les autorités ont été surprises de l'organisation et des capacités de l'ennemi. Les soldats s'attendaient en effet à un modèle basé sur une intifada (une révolte contre un régime étranger jugé comme oppresseur) bien connu des soldats dans le cadre de la lutte en Palestine. Ils se sont cependant retrouvés face à des groupes entrainés, armés de matériel lourd (missiles antichar par exemple) et déterminés. Les habitudes stratégiques et opérationnelles des soldats, habitués à une grande asymétrie dans le cadre de la guerre irrégulière menée par les

Palestiniens, ont été source de nombreuses pertes pour l'armée israélienne. Israël ne s'attendait pas à se retrouver confronté à ce que l'on pourrait qualifier d'armée irrégulière ; la vision était majoritairement scindée entre conflit irrégulier et asymétrique (intervention en Palestine) ou régulier (guerre de haute intensité face à ses voisins).[55]

Par cet exemple, la guerre hybride semble davantage se définir dans l'emploi de capacités et de compétences jusqu'alors propres aux États et armées régulières dans un contexte d'irrégularité (guérilla, soutien de la population, ennemi non identifiable, non-respect des codes de guerre par l'ennemi...). Ici, la guerre hybride rend difficile les opérations pour les armées régulières ; l'ennemi qui garde une irrégularité et qui se dissimule au sein d'une population diminue l'avantage technologique d'une armée et tend à réduire l'asymétrie (impossibilité de faire des frappes aériennes et obligeant une intervention terrestre exposant les soldats engagés sur le terrain par exemple).

L'exemple de l'État islamique en 2014

La lutte contre l'État islamique a également été perçue comme relevant d'une guerre hybride. En 2014, le président américain Barack Obama déclarait ainsi que l'État islamique *« est un challenge hybride, ce n'est pas un simple réseau terroriste, ils ont des ambitions territoriales et font usage de stratégie et tactique semblable à une armée. » [Barack Obama dans une interview donné à Steve Croft pour Central Broadcasting Networ, 2014]*. En effet, pour parvenir à son aspiration territoriale, l'État islamique a usé de stratégie militaire lors de batailles face aux armées régulières en Irak ou en Syrie, mais également d'actions terroristes contre la population. La population a également servi de bouclier humain contre les frappes de la coalition internationale. La communauté internationale a également été surprise de découvrir une organisation terroriste qui disposait d'une administration sur les territoires conquis et qui contrôlait grandement les populations. De plus, grâce à ses conquêtes territoriales, le groupe a dérobé les armes des armées conventionnelles s'étant repliées, augmentant alors leur arsenal. L'utilisation de technologies nivelantes (drones explosifs par exemple) a également été un nouveau défi pour les forces armées faisant face à l'État islamique. Enfin, l'État islamique a su tirer profit du cyberespace en termes de communication et de propagande, menant une véritable guerre de l'information avec les puissances étrangères.[56]

L'exemple de la guerre du Donbass depuis 2014

Dans le cadre de la guerre du Donbass, l'hybridité de la guerre se retrouve dans un premier temps sur la question de la guerre par procuration. En effet, les milices armées pro-russes, bien que n'étant pas directement rattachées à la Russie, peuvent recevoir un soutien (renseignement, matériel...) officieux de la part de la Russie, qui y gagne en défendant des milices qui étendent sa sphère d'influence au détriment de l'Union Européenne. L'hybridité se retrouve ici dans la porosité entre guerre ouverte et guerre couverte menée par la Russie qui, faute de preuves formelles de son implication,

peut nier toute implication devant la communauté internationale. Cette guerre s'est également jouée sur le plan politique et diplomatique. La Russie a en effet indiqué vouloir défendre et protéger les populations russophones d'un coup d'État anticonstitutionnel en Ukraine et ont pu jouer la carte du droit à l'autodétermination d'un peuple au travers d'élections, comme ce fut le cas pour l'annexion de la Crimée. La Russie a également contrôlé le domaine de l'information pour justifier ses actions au sein de sa sphère d'influence et rallier les populations pro-européennes à la cause russe (argument d'une Europe fasciste pour utiliser la mémoire de la Seconde Guerre mondiale, argument d'une action humanitaire pour faire respecter les droits de l'Homme envers les populations russophone en Ukraine...). Les médias occidentaux ont également subi une vague de commentaires de propagande pro-russe sur leurs publications. Toujours sur le plan international et informationnel, des médias internationaux russes ont émergé (chaine de télé RT, journal Sputnik) afin de diffuser la « vérité alternative » russe et gagner de l'influence auprès des populations occidentales.[57]

La guerre hybride est donc une notion encore floue, très large, qui se définit aujourd'hui avant tout par des exemples et donc un choix arbitraire pour qualifier un conflit d'hybride ou non. Cependant, les conflits armés voient leurs formes changer, obligeant les armées régulières à s'adapter ; la guerre hybride, bien que floue, permet donc d'approcher cette nouvelle réalité. Aujourd'hui, cette réalité peut aussi bien s'illustrer par l'action de l'État islamique au Moyen Orient qu'avec les guerres en Ukraine face aux séparatistes pro-Russes et l'avènement de nouveaux milieux de confrontation tels que le cyberespace.

3.1.2 La cyberguerre, un concept plausible ?

Le concept de la cyberguerre tient son origine d'un constat indéniable : les révolutions technologiques se retrouvent mobilisées au profit de la guerre ; machine à vapeur qui a influencé les guerres civiles américaines, la guerre de 1870 ainsi que la Première Guerre mondiale, apparition de l'essence qui développe les véhicules engagés dans les batailles (camions, chars, avions) ou encore l'utilisation du nucléaire au profit des armes. L'émergence du domaine cyber n'a pas échappé à cette tradition : aujourd'hui les systèmes d'armes sont imprégnés de systèmes d'information, les avions de combat disposent de systèmes d'aide à la décision, les futurs bâtiments de la Marine Nationale (Frégate de Défense Intermédiaire ou FDI) se basent sur le numérique au point d'être qualifiés de « cyberfrégate ». Pour les armées, le cyber représente donc une avancée majeure dans l'évolution des capacités. Néanmoins, il offre une nouvelle surface d'attaque (virus clouant les avions au sol, désactivant les systèmes d'armes d'une FDI...).

Le cyber a également révolutionné l'idée du commandement des opérations. Avant les années 1990, il était commun de parler de *Command and Control (C2)* pour parler du commandement dans l'armée. Avec l'informatisation des services de commandement, le C2 est devenue C4 : *Command, Control, Communication and Computer* puis

C4ISR (*Command, Control, Communication, Computern, Intelligence, Surveillance and Reconnaissance*) et enfin C4ISTAR (Computerized Command, Control, Communications, Intelligence, Surveillance, Target Acquisition and Reconnaissance). Le cyber a donc non seulement révolutionné les capacités sur le terrain, au même titre que d'autres révolutions technologiques, mais également la conception du commandement et la façon dont peuvent être menées les opérations.[58]

Au vu de sa prédominance dans les armées modernes et dans nos sociétés, le cyber est également perçu comme un potentiel nouveau domaine de lutte, au même titre que les domaines terrestre, aérien et maritime.[59]

En 2010, le département américain de la Défense a émis une note définissant la cyberguerre comme *« un conflit armé conduit totalement ou partiellement par des moyens cyber, [soit] des opérations militaires menées pour interdire à l'ennemi l'utilisation des systèmes du cyberespace et de ses armes au cours d'un conflit ». [Joint Terminology for Cyberspace Operations, Department of Defense, 2010]*.[60] Cependant, il semble important d'ajouter à cette définition que les acteurs de la cyberguerre peuvent être étatiques comme non étatiques.[61] Les acteurs non étatiques peuvent alors être rattachés à un État qui cherche à mener des actions sous couvert d'anonymat afin de ne pas en porter la responsabilité sur la scène internationale. Bien que les preuves manquent, comme souvent quand il s'agit du domaine cyber, cela peut s'illustrer avec les cyberattaques présumées des Russes, menées envers l'Estonie en 2007. Sans être forcément commanditées et dirigées par l'État russe, celui-ci a laissé faire ces cybercriminels patriotes. En ce sens, la cyberguerre est une composante majeure de la guerre hybride, permettant à un État d'agir sous couvert, au travers d'acteurs non conventionnels.

Si la cyberguerre est envisagée par des États, celle-ci se doit de respecter un cadre juridique, conforme au droit de la guerre. En 2013, un groupe d'experts de l'OTAN a rédigé le *Manuel de Tallin* qui transpose le droit internationnal aux concepts de cyberguerre. Le manuel définit alors une cyberattaque militaire comme *« une agression armée lorsque l'emploi de la force atteint un seuil élevé en termes de degré, de niveau d'intensité et selon les effets engendrés : pertes en vies humaines, blessures aux personnes ou des dommages aux biens. » [Manuel de Tallin, OTAN, 2013]*.[62] En caractérisant ainsi l'usage du cyber comme une arme, les États peuvent faire valoir leur droit à la légitime défense, conformément à l'article 51 de la Charte des Nations Unies. En effet, cet article dispose qu' *« Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée [...]. » [extrait de l'article 51 de la Charte des Nation Unies]*.

Devant une audition du Sénat en juin 2019, le chef d'État-Major des Armées a rappelé que pour la France, le cyber est une arme d'emploi *« pour la défense de nos intérêts et de notre souveraineté. » [CEMA, audition devant le Sénat, juin 2019]*. Dans un rapport d'information de 2011 sur la cyberdéfense, [63] le Sénat caractérise trois

moyens d'action pour la guerre informatique :

- la guerre *contre* l'information qui vise à impacter le critère d'intégrité des données et de disponibilité d'un système.
- la guerre *pour* l'information qui vise le critère de confidentialité des données.
- la guerre *par* l'information qui constitue le volet de propagande et de guerre de l'information.

Le concept de cyberguerre ne fait cependant pas l'objet de consensus. Bien qu'ils soient définis et encadrés par un droit international, certains ne voient pas en ce concept une réalité opérationnelle. Dans un article intitulé *« Cyberwar will not take place »*, Thomas Rid évoque l'idée que le domaine cyber n'est qu'un domaine d'action parmi les autres et n'est pas à lui seul une finalité en termes d'affrontement. Ainsi, le cyber serait davantage un domaine de lutte en soutien aux opérations ayant lieu dans le monde physique (renseignement, appui d'un assaut en réduisant les capacités adverses, guerre de l'information...). Pour défendre cette idée, il évoque le fait qu'aucune cyberguerre n'a encore eu lieu malgré les technologies existantes et qu'aucune cyberattaque n'a fait de victimes humaines (il a fallu attendre 2020 et le décès d'une patiente en Allemagne pour qu'un concours de circonstance dramatique viennent invalider cet argument). Ainsi, il semblerait plus judicieux de parler d'un élargissement des domaines de la guerre et d'introduire le concept de cyberopération plutôt que de parler de cyberguerre. En ce sens, la seconde édition du manuel de Tallin publié en 2017 ne parle plus du droit applicable dans la cyberguerre mais appliqué aux cyberopérations afin de tenir compte des reproches de terminologie qui ont été émis envers la première édition.[65]

Le risque cyber est cependant bien intégré au sein des États tels que la France. Des doctrines et des stratégies sont édictées depuis les années 2010 (voir partie 3.3 - Regards croisés entre les doctrines cyber des États) afin de faire face à ce risque qui, bien que potentiellement mal défini d'un point de vue de la terminologie et de la conceptualisation, est une réalité.

3.1.3 Conclusion

La cyberguerre ne semble pas être un concept pertinent ; celle-ci n'existe pas par elle-même et ses conséquences ne sont pas une finalité opérationnelle. Le terme de cyberopération semble plus pertinent afin de parler de l'émergence du domaine cyber au sein des armées et stratégies de défense en plaçant le domaine cyber en parallèle des trois autres domaines traditionnels (terre, air, mer). Ainsi les cyberopérations sont dans la continuité et en soutien des opérations traditionnelles. Celles-ci prennent sens dans le concept de guerre hybride, qui bien que n'étant pas défini clairement, illustre une réalité en termes de changement des opérations militaires, notamment dans le cadre de la guerre contre des groupes terroristes et séparatistes. Le concept des cyberopération permet également de concrétiser l'utilisation du cyberespace à des fins opérationnelles pour lutter contre les groupes terroristes et séparatistes.

3.2 Les cyberopérations : un nouvel outil pour les groupes terroristes et les États

3.2.1 Les cyberopérations au service de la guerre par l'information et des actions civilo-militaires

La guerre par l'information peut avoir plusieurs objectifs pour les groupes terroristes. La forme la plus basique se retrouve dans la propagande et les éventuelles opérations d'embrigadement. La guerre par l'information peut également avoir pour objectif la désinformation, soit à but stratégique (induire l'ennemi en erreur par la transmission de fausses informations, on retrouve un exemple historique dans le plan Jaël lors de la Seconde Guerre mondiale) ou politique (comparable à une certaine forme d'ingérence pour déstabiliser un État, cela peut s'illustrer avec la prétendue désinformation russe lors des élections américaine de 2016).

Face à des luttes contre le terrorisme qui prennent davantage l'aspect d'une guerre, la communication et la maitrise de l'information sont cruciales au sein des différents acteurs de ces conflits. L'importance de la maitrise de l'information dans une guerre peut s'illustrer au travers de la guerre du Vietnam et de son dénouement. En effet, à la suite de la pression médiatique influençant l'opinion publique, la décision a été prise de retirer les troupes du pays. Ainsi, sans perdre la guerre sur le champ de bataille, les États-Unis, première puissance militaire mondiale, ont perdu cette guerre à cause du domaine de l'information. Aujourd'hui, avec la présence du cyberespace, l'information circule encore plus vite et atteint davantage de personnes. L'information existe également sous différents points de vue et chaque acteur d'une guerre peut se vanter de détenir la vérité et diffuser celle-ci au travers d'une sphère d'influence pour contrôler l'opinion de la population et/ou des combattants. La désinformation au sein de la sphère d'influence adverse s'illustrera par de la propagande et de l'embrigadement au niveau des groupes terroristes. Pour les États luttant contre ces groupes terroristes l'effet recherché sera de diviser les insurgés, de rallier les indécis et éventuellement de dissuader les combattants ennemis.[66]

L'État islamique a très vite compris l'importance de la guerre par l'information. En effet, au vu de leur ambition de contrôler des territoires et leurs populations, la communication et l'établissement d'une image positive de l'organisation se sont révélés indispensables. En effet, selon les estimations, l'État islamique aurait eu une population de plus de 10 millions de personnes à contrôler. Sans le soutien d'une partie de cette population, maintenir le califat nouvellement installé aurait été impossible. L'organisation terroriste a alors mis en œuvre une stratégie de communication par des mediums aussi bien physiques (distribution de tracts, événements en présentiel) que virtuels au travers du cyberespace (présence sur les réseaux sociaux, magazine...). L'objectif pour le groupe était de montrer à la population le côté fonctionnel du califat, en opposition avec les conflits armés de haute intensité qui avaient lieu aux frontières de ce même califat. Cet aspect diffère du cyberdjihadisme (qui demeure néanmoins

une composante de la guerre par l'information) essentiellement tourné vers l'extérieur pour faire rayonner l'organisation et recruter ; il s'agit-là de conforter ses positions en interne et d'occuper le domaine informationnel pour éviter que celui-ci soit accaparé par l'ennemi.

La guerre par l'information, visant notamment les populations civiles, se retrouve également dans le concept d'opération psychologique (PSY OPS). Les PSY OPS peuvent inclure des cyberopérations afin de lutter contre la désinformation et/ou pour tenter de légitimer la présence d'une force étrangère sur un territoire. Cette communication peut s'axer autour de la valorisation des actions-civilo militaires et peut ainsi se définir comme une offensive face aux groupes terroristes dans le domaine de la guerre par l'information. PSY OPS et action civilo-militaire sont intimement liées, les PSY OPS étant généralement permises grâce au climat de confiance construit au travers des actions civilo-militaires.[67]

La lutte contre le terrorisme, à l'image de l'opération Barkhane dans laquelle la France est engagée depuis 2014 contre les groupes armés terroristes en bande sahélo saharienne, s'effectue également autour d'actions civilo-militaires. Ces actions ont pour vocation de faciliter l'intégration des forces armées parmi les populations civiles afin de faciliter l'accomplissement des missions militaires. Dans la lutte contre le terrorisme, l'objectif n'est pas seulement de vaincre militairement l'ennemi mais également de laisser un pays viable pour éviter tout retour de groupes terroristes armés profitant de la désorganisation et du chaos environnant pour prendre position. Cependant, l'expérience a montré, notamment au travers de la guerre d'Afghanistan, que ces actions en faveur de la reconstruction du pays ne devaient pas intervenir après les opérations militaires mais en parallèle.[68]

Concrètement, sur le terrain, le volet cyber des PSY OPS va s'axer autour de la communication sur les nouveaux canaux qu'offre le cyberespace. Dans le cadre de l'opération Barkhane, l'objectif est essentiellement de lutter contre la désinformation qui alimente un sentiment anti-français au sein de la population. Or, dans un conflit asymétrique où les soldats sont au contact de la population et que celle-ci dispose d'informations précieuses pour le succès des opérations, la défiance de cette dernière complique l'action militaire.

Par exemple, en novembre 2019, des fausses informations indiquaient que l'armée française était responsable d'une attaque envers une base de l'armée nigérienne car elle soutenait les groupes armés terroristes de la région. Les publications ont été très vite massivement partagées et la population locale a alors accusé les forces françaises d'être de nouveaux colonisateurs. Une telle campagne de désinformation peut avoir des effets catastrophiques ; défiance de la population, recrutement par les groupes terroristes, soutien de la population aux terroristes, etc.[69]

Pour les forces en présence, il est donc indispensable de collaborer avec les autorités locales afin de lutter contre la désinformation et de communiquer, autant dans le monde physique que sur le cyberespace, autour des actions civilo-militaires afin de gagner la confiance de la population et participer à la stabilisation civile du théâtre d'opération.

Pour les forces armées luttant contre le terrorisme, la capacité à mener des cyberopérations répond à la capacité de faire face à la guerre par l'information sur deux aspects :

— Premièrement, dans un aspect défensif, faire face à la désinformation visant à discréditer la force militaire auprès de la population.

— Deuxièmement, dans un aspect offensif, occuper le cyberespace afin de communiquer et appuyer les actions civilo-militaires qui favorisent le contact avec la population, permettant de faciliter les opérations militaires.

3.2.2 Une guerre sur fond de cyberopérations : l'exemple ukrainien

La guerre du Donbass depuis 2014 et la crise ukrainienne associée illustrent parfaitement la guerre hybride et l'usage de cyberopérations. Ces conflits opposent l'État ukrainien à des séparatistes pro-russes, jugés comme terroristes par le gouvernement ukrainien. Dans cet exemple de guerre hybride, deux puissances étatiques s'affrontent indirectement (Ukraine et Russie) du fait du soutien de la Russie aux séparatistes qui font face aux forces régulières ukrainiennes. Dans le cadre de cette crise aux multiples enjeux, de nombreuses cyberopérations ont été menées afin de soutenir les opérations physiques et gagner la guerre de l'information à l'international.

Pour les séparatistes pro-russes, cette guerre par l'information via le cyberespace avait pour principal objectif de rallier la population non combattante à la cause, ou du moins de ne pas avoir la désapprobation de la population, ce qui aurait entrainé un désavantage sur le terrain pour les opérations physiques, qui restaient la priorité aux yeux des séparatistes.

Pour ce faire, les séparatistes se sont imposés comme les protecteurs des populations face à un régime ukrainien coupable d'exactions envers les populations civiles. De plus, en imputant les origines du conflit au gouvernement ukrainien, les séparatistes ont su diriger la colère issue de la guerre présente chez les habitants envers les troupes ukrainiennes et non séparatistes.

Les séparatistes ont également véhiculé l'idée d'une guerre menée par un mouvement populaire que chacun pouvait rejoindre. Cette diffusion de la vision de la guerre mais aussi géopolitique (combat contre une Ukraine capitaliste pro-américaine) a permis d'agrandir les rangs autant en termes de combattants que de sympathisants,

permettant d'avoir un soutien logistique et/ou organisationnel pour appuyer les combattants. Le financement dans une guerre étant essentiel, les séparatistes ont également usé du cyberespace pour lever des fonds.

Les séparatistes pro-russes ont également occupé le terrain informationnel au-delà des populations civiles peuplant les territoires occupés. Ces cyberopérations à portée informationnelle visaient notamment les familles des militaires ukrainiens afin de les dresser contre le conflit. Pour ce faire, les séparatistes ont diffusé des prétendues preuves d'exactions commises par l'armée ukrainienne et ils ont également communiqué autour du succès militaire chez les séparatistes. Les familles des militaires, ne soutenant plus la cause et craignant pour la vie de leurs proches sur le front, ont alors grandement influé sur le moral des troupes ukrainiennes. Affaiblir le moral des combattants ukrainiens a permis de faire baisser le niveau de ténacité et d'engagement des hommes sur le front, facilitant les opérations au sol pour les séparatistes.[70]

La guerre physique en Ukraine, à l'aspect très traditionnel, parfois illustrée par une guerre de tranchées, est néanmoins très influencée par des cyberopérations, si ce n'est facilitée par ces cyberopérations en ce qui concerne les séparatistes.

Face à cette guerre par l'information, l'armée ukrainienne n'a eu d'autre choix que de réagir. Dans un reportage d' « Enquête Exclusive » tourné en 2020, des journalistes ont suivi un commando des forces spéciales ukrainiennes en pleine cyberopération. L'objectif de ces hommes était de contrer la propagande pro-russe portée par les séparatistes au travers d'une guerre des ondes radio. Le commando, après être rentré en territoire ennemi, avait pour objectif de déployer du matériel permettant de brouiller une émission de radio pro-russe pour y diffuser à la place une émission ukrainienne.[71]

Cet exemple illustre bien le champ d'action des cyberopérations contre des groupes séparatistes dans une guerre hybride. Des forces spéciales sont en effet employées pour influencer la population et gagner son soutien à l'encontre des forces séparatistes au travers du cyberespace (le domaine électromagnétique englobant la radio pouvant être rattaché au cyberespace au vu de l'interdépendance des deux domaines).

Sans être le fruit direct des séparatistes, l'Ukraine connait depuis 2014 une prolifération des cyberattaques à l'encontre de ses systèmes d'information. Ces cyberattaques permettent de mieux situer la place des cyberopérations au sein du concept de guerre hybride ; les acteurs (séparatistes, États, groupes criminels) sont difficilement identifiables, tout comme les liens entre eux.

Cela s'illustre parfaitement avec les événements du 27 juin 2017 et l'assassinat d'un officier du renseignement ukrainien, chargé de récolter des preuves de l'implication russe dans la guerre du Donbass. Cet assassinat, non revendiqué, provoqué par l'explosion de la voiture de l'officier, a été considéré comme un attentat terroriste par les autorités ukrainiennes. Quelques heures après, des milliers de systèmes d'information (ordinateurs d'entreprises ou de ministères, opérateurs de télécommunications,

distributeurs de billets...) sont paralysés par un logiciel malveillant : *NotPetya*. NotPetya aurait infecté près de 30 % des systèmes d'information du pays.[72] L'Ukraine mettra plusieurs jours pour retrouver ses capacités après cette attaque d'ampleur qui semble liée à l'attentat contre l'officier du renseignement quelques heures plus tôt, d'autant plus que selon certaines sources l'heure de déclenchement du logiciel malveillant a été inscrite dans le code. Cette cyberopération menée en parallèle à l'action physique semble avoir été orchestrée par un groupe de cybercriminels pro-russes. Son objectif était visiblement de créer la confusion et semer la panique dans le pays, mais également d'impacter considérablement les capacités cyber de l'Ukraine. Cette cyberattaque ne peut cependant être qualifiée de cyberterrorisme ; aucune victime physique n'est à déplorer, elle n'est pas revendiquée par les séparatistes et ils n'en sont pas à son origine, elle est tout au plus commanditée par ces derniers (bien qu'en vérité il semble plus que ce soit le gouvernement Russe qui ait orchestré l'attentat et la cyberattaque).

L'Ukraine a également fait face à d'autres cyberattaques de grande ampleur revendiquées par des séparatistes pro-russes. Par exemple, en 2014, une cyberattaque a paralysé les systèmes liés à l'élection présidentielle quelques jours avant la date du scrutin. En 2015, une cyberattaque provoque la déconnexion électrique de centrales, privant plusieurs dizaines de milliers de personnes de courant pendant que d'autres cyberattaques ont paralysé les services de secours. L'objectif de ces cyberopérations (plusieurs cyberattaques coordonnées et ciblées, avec parfois des opérations physiques en parallèle) est de déstabiliser le pays et de contrecarrer sa légitimité à gouverner, tout en affectant le moral des troupes engagées sur un front physique et les capacités opérationnelles dont il peut disposer. En effet, les systèmes d'information militaires peuvent être également impactés par ces cyberattaques qui s'orientent essentiellement sur la perte du critère de disponibilité, voire de l'intégrité des données.

En 2017, dans le but de dissuader les troupes ukrainiennes, une campagne de cyberharcèlement a été menée par les séparatistes. Les soldats ont reçu simultanément des SMS les incitant à ne pas prendre part au combat au risque d'y perdre la vie. Ce n'était pas la première fois que les séparatistes menaient une cyberopération par la diffusion de SMS ; en 2015, de faux messages d'alerte, voire de menaces aux populations civiles, ont été envoyés afin de déstabiliser la population et réfréner toute résistance.

Pour parvenir à mener ces cyberopérations de propagande et de déstabilisation à la fois chez les civils et chez les militaires, les séparatistes ont déployé des antennes de télécommunication afin de diffuser les messages à tous les smartphones à portée. Selon certaines sources, du matériel plus poussé (IMSI Catchers), permettant un meilleur ciblage des victimes des cyberopérations, a été fourni par la Russie aux séparatistes. Un ciblage plus fin permet en effet d'avoir plus de répercussions auprès des cibles.[73]

L'Ukraine est un bon exemple de la guerre hybride, tant par l'utilisation de groupes terroristes séparatistes par une nation pour agir indirectement, que par l'usage de cyberopérations menées en soutien aux opérations physiques. Dans ce cas, les séparatistes

n'ayant pas les compétences pour mener les cyberopérations, ils travaillent de concert avec des groupes de cybercriminels.

L'effet final recherché par ces cyberopérations est essentiellement le ralliement de la population à la cause, ou du moins sa non-résistance. De plus, en déstabilisant les infrastructures du pays et en dissuadant les militaires ukrainiens, les cyberopérations facilitent la progression des séparatistes.

Certains voient en l'Ukraine un terrain d'essai russe, autant sur le plan de la guerre hybride que des cyberopérations (à la fois l'aspect technique, à savoir la réalisation de cyberattaques, qu'organisationnel afin d'en évaluer les impacts et retombées sur le terrain).[74]

3.2.3 Conclusion

Le cyberespace permet aux groupes terroristes mais également aux forces luttant contre eux de mener des cyberopérations facilitant les opérations dans le monde physique (voir annexe Annexe C - Exemples d'emploi de la LIO au niveau tactique et au niveau stratégique). Cela peut s'illustrer au travers des PSY OPS et actions civilo-militaires de l'armée française dans l'opération Barkhane ou bien dans les cyberopérations des séparatistes pro-russes en Ukraine. Dans les deux cas, la population civile est au centre des intérêts afin d'obtenir le soutien ou a minima éviter la création d'un mouvement de résistance. Les cyberopérations constituent donc un nouvel éventail d'actions possibles, tant défensives qu'offensives, dans la lutte contre le terrorisme.

3.3 Regards croisés entre les doctrines cyber des États

3.3.1 Doctrine Française

Le livre blanc sur la défense et la sécurité nationale de 2008 plaçait la sécurité des systèmes d'information comme un élément de souveraineté nationale. Afin de structurer la défense des systèmes d'information, le gouvernement a créé en 2009 l'Agence nationale de la sécurité des systèmes d'information (ANSSI). En 2011, la France se dote pour la première fois d'une stratégie portant sur la sécurité des systèmes d'information.[75]

La stratégie présente s'articule autour de quatre objectifs :

— *« Être une puissance mondiale de cyberdéfense »* ; le document indique notamment que des États ou des groupes terroristes pourraient s'attaquer à des infrastructures vitales de la nation, rendant indispensable la dotation d'une capacité de cyberdéfense.

— *« Garantir la liberté de décision de la France par la protection de l'information*

de souveraineté » ; cet objectif vise à assurer le maintien des communications et des systèmes d'information essentiels, peu importent les circonstances, pour être résilient à toute tentative de désorganisation.

— *« Renforcer la cybersécurité des infrastructures vitales nationales »* ; l'objectif poursuivi est d'assurer la disponibilité et l'intégrité des systèmes d'information nécessaires au bon fonctionnement des OIV.

— *« Assurer la sécurité dans le cyberespace »* ; cet objectif a pour finalité d'assurer la sécurité de tout citoyen ou entreprise face aux nouvelles menaces cyber qui émergeaient au début des années 2010.

Le champ de l'action de l'ANSSI est essentiellement orienté vers le domaine civil et uniquement composé d'un volet défensif. Également, en 2011, il n'y avait pas de notion de guerre par l'information sur le cyberespace ou de lutte contre le cyberdjihadisme. Ces aspects sont donc absents dans ce document.

Pour combler le manque de prise en compte du domaine cyber dans les armées, le COMCYBER est créé début 2017 et a pour vocation de conduire les opérations de cyberdéfense à portée militaire. La loi de programmation militaire 2019-2025 prévoit plus de 4 000 cybercombattants dans les rangs de l'armée française afin de faire face à la recrudescence des cybermenaces envers les systèmes de l'armée.

Afin d'accompagner ces institutions, en 2019, la ministre des Armées Florence Parly a affirmé que *« la France emploie et emploiera l'arme cyber dans ses opérations militaires » [Florence Parly, ministre des Armées, 2019]*. Cette déclaration est intervenue lors de la présentation de deux doctrines : l'une liée à la lutte informatique offensive [6] (LIO) et l'autre à la lutte information défensive[76] (LID).

Doctrine française en matière de LID

La doctrine en matière de LID se place en cohérence avec les missions définies par la revue stratégique de cyberdéfense de 2018. Cette dernière s'axe autour de six missions principales vis-à-vis des cybermenaces et des cyberattaques ; la prévention, l'anticipation, la protection, la détection, la réaction et enfin l'attribution.

Pour le ministère des Armées, la LID a pour objectif de maintenir sa liberté d'action. En des termes plus concrets cela signifie que les forces physiques doivent pouvoir mener à bien leurs missions sous une cyberattaque. La LID constitue donc une résilience face aux cybermenaces qui peuvent entraver les forces. En effet, les systèmes d'information et de communication sont essentiels dans la chaine de commandement mais également sur le terrain au sein des forces (avions, bâtiments de la Marine, programme SCORPION de l'armée de terre).

La doctrine rappelle également que la sécurité des systèmes d'information tient de la coopération entre les différents acteurs (ANSSI, COMCYBER, services de renseignement...). En effet, la doctrine LID souligne qu'une attaque visant le système militaire peut profiter des faiblesses d'un ministère connexe ou d'un industriel proche du sec-

teur de la défense. Ainsi, dans un souci d'efficience, la coopération civils-militaires est indispensable.

Doctrine française en matière de LIO

Les éléments de doctrine publique en matière de LIO reconnaissent que le cyber est un nouveau moyen de mener la guerre sans pour autant bouleverser totalement les principes de la guerre. Cette vision retranscrit donc les éléments précédemment abordés : la cyberguerre n'existe pas en soi, il y a des cyberopérations au profit d'une guerre ou d'une conflictualité permanente (espionnage entre États par exemple). La finalité de la LIO est donc bel et bien d'utiliser le cyberespace comme soutien aux opérations militaires classiques.

L'utilisation de la LIO permet de garantir la souveraineté nationale et d'obtenir l'avantage sur des théâtres d'opérations physiques par une multiplication des effets (amplification, amélioration, complétion des opérations physiques). Sans offrir une doctrine sur la lutte contre la manipulation d'informations, la doctrine LIO met également cet aspect en avant, reconnaissant son importance en qualifiant ces manipulations comme pouvant être nuisibles pour les opérations militaires.

Pour les armées, la LIO permet d'obtenir du renseignement, de neutraliser ou d'affaiblir les capacités adverses et/ou de déception d'un ennemi (altération de l'intégrité des systèmes d'information). La LIO est également un moyen d'appuyer la LID en attaquant la source d'une cyberattaque à l'encontre d'un système d'information de l'armée.

La France montre néanmoins un fort attachement à l'éthique de l'emploi de ces nouvelles armes. La doctrine rappelle en effet les risques d'effet de bord d'une cyberattaque à cause de l'hyperconnectivité du cyberespace et du risque d'inconnu en termes de configuration chez l'ennemi. Le risque est également de fournir une arme à l'ennemi (récupération du code d'un logiciel malveillant par exemple). Ainsi, pour les armées, la LIO doit faire preuve de vigilance afin d'éviter tout risque de dommages collatéraux (notamment civils), de compromission dans le cadre d'opérations de nature secrète et/ou de détournement de l'attaque.

De futures doctrines pour faire face guerre par l'information

Pour lutter contre la propagande de l'État islamique, le commandant du COMCYBER a expliqué que les armées ont *« ciblé tout leur appareil de propagande, identifié où étaient localisés les serveurs, pénétré ces serveurs, effacé les données, et bloqué ces serveurs pour que la propagande ne puisse plus être diffusée » [général Didier Tisseyre, commandant du COMCYBER, 4 mars 2020 devant l'Assemblée nationale]*.[77] Ces cyberopérations offensives, relevant de la LIO, avaient pour objectif de lutter contre le cyberdjihadisme et d'endiguer les manœuvres de recrutement.

De telles manœuvres ne sont cependant pas toujours possibles sur le cyberespace. Aujourd'hui apparait le concept de Lutte Informatique d'Influence (L2I) visant à oc-

cuper le cyberespace pour contrer les opérations de désinformation. La France devra donc probablement se doter d'une doctrine de L2I pour compléter son arsenal cyber dans la lutte contre le terrorisme.

3.3.2 Doctrines de pays étrangers

Afin de comparer les visions quant à l'usage du domaine cyber dans le cadre de la guerre (ou d'une posture permanente en termes défensifs ou offensifs pour le renseignement), nous allons parcourir les doctrines de pays qui prônent l'usage du cyber dans leurs armées et ont les moyens de mettre en place leurs ambitions. Ces pays sont la Russie, souvent accusée de cyberattaques contre des pays occidentaux, les États-Unis d'Amérique, souvent vus comme précurseurs dans le domaine cyber, et enfin Israël, un pays en guerre continue contre la Palestine et sous la menace de guerre avec les pays voisins, qui cherche par conséquent à développer ses capacités militaires afin de garder l'avantage.

Il aurait pu être intéressant d'ajouter la Chine à cette étude. Ce pays connaît en effet un fort développement de ses capacités militaires depuis quelques années et sa maitrise des nouvelles technologies de l'informatique et des communications a connu un essor sans précédent. Bien que la Chine ne soit pas engagée dans des conflits, les accusations d'actes d'espionnage au moyen de cyberarmes sont nombreuses. Les cyberopérations offensives sont donc très bien maitrisées mais il n'existe aucune doctrine publique permettant de se renseigner davantage sur le sujet, tant sur le plan défensif qu'offensif.

Doctrine des cyberopérations en Russie

Fin 2016, la Russie s'est dotée d'une doctrine de cybersécurité afin de faire face à l'augmentation de la menace cyber mais également de l'influence étrangère. Les éléments publics publiés au travers de cette doctrine s'apparentent essentiellement au domaine de la LID et de la L2I.

Selon cette doctrine, la Russie craint principalement les cyberopérations occidentales visant la population russe en termes d'influence, qui s'attaqueraient selon elle aux « valeurs culturelles et spirituelles » du pays. Dans un pays autoritaire cela peut également signifier une meilleure lutte contre les débuts insurrectionnels pouvant avoir lieu, les printemps arabes ayant démontré le rôle des réseaux sociaux dans les révolutions. L'aspect de maitrise de l'influence étrangère semble donc également recouvrir des aspects de sécurité intérieure.[78]

Dans la notion de conflictualité permanente entre la Russie et des pays occidentaux, la doctrine cherche également à garantir les critères DIC de ses systèmes et d'être imperméable à l'espionnage.

Cependant, contrairement à la France, la doctrine ne prend pas en compte les acteurs privés civils pourtant nombreux, et qui assurent la cybersécurité des institutions russes.[79]

En ce qui concerne le domaine offensif, celui-ci n'est pas évoqué. Cependant, l'implication russe dans des cyberopérations (espionnage, implication dans la guerre du Donbass, cyberattaques...) est régulièrement pointée du doigt. Néanmoins, au vu des éléments en notre possession, il semblerait que la stratégie offensive s'appuie notamment par la coopération de groupes de hackers pro-russes. Par l'implication de groupes civils non rattachés directement au pays, la Russie pourrait chercher à nier toute implication directe en renvoyant la responsabilité sur des individus non liés à l'État. Cette stratégie peut se rattacher au concept de guerre hybride où les acteurs et les relations entre ces derniers sont flous. Le cyberespace facilitant l'anonymat, c'est un domaine idéal pour y appliquer cette stratégie de guerre hybride afin d'y mener des cyberopérations sans avoir à en assumer les éventuelles conséquences sur la scène internationale faute de preuves de l'attribution et/ou de l'implication du gouvernement dans l'organisation de la cyberattaque.

Doctrine des cyberopérations aux États-Unis d'Amérique

L'aspect défensif était couvert, depuis les attentats du 11 septembre 2001, par le département de la sécurité intérieure qui a pour mission d'assurer la sécurité du territoire national sur tous les domaines. Une division se concentrant sur le cyber a complété le département de la sécurité intérieure en 2003 afin de répondre plus spécifiquement aux nouvelles menaces. Le FBI est aussi impliqué au travers de ces *Cyber Action Team*, notamment pour assurer les enquêtes après une cyberattaque et assurer le lien sur les questions cyber avec les entreprises importantes américaines.

La NSA s'occupe de l'aspect défensif et offensif du département de la défense. Afin de coordonner les opérations offensives menées par la NSA au profit des autres armées, un commandement de cyberdéfense a vu le jour en 2010, l'USCYBERCOM, chargé de planifier et conduire les cyberopérations, tant défensives qu'offensives, au profit du département de la défense.

Les États-Unis d'Amérique disposent de doctrines défensive et offensive qui prennent également en compte l'aspect d'influence comme une composante pouvant servir les intérêts militaires mais dont il faut également se protéger. Tout comme la France, les aspects défensif et offensif sont perçus comme étant complémentaires, une offensive pouvant permettre de mettre fin à une cyberattaque subie.[80]

Contrairement à la France, les États-Unis d'Amérique ne disposent pas d'une agence nationale civile en charge de la cybersécurité des infrastructures critiques du secteur privé. En 2010, il a alors été décidé que la NSA soutiendrait le département de la sécurité intérieure afin de participer à la cybersécurité des infrastructures critiques. Les États-Unis ont également procédé à l'identification de leurs infrastructures critiques, à l'image des OIV en France. Ainsi, comme en France, la coopération entre le

secteur privé et public est importante afin d'assurer une efficience à tous les niveaux. De plus, bien que relevant davantage de la politique internationale, contrairement à la France, les États-Unis d'Amérique n'hésitent pas à faire part des cyberattaques qu'ils subissent et à accuser des États sans forcément avoir de preuves concrètes.[81]

Enfin, les États-Unis d'Amérique sont connus pour avoir mené la cyberopération offensive contre l'Iran visant à retarder le programme d'acquisition de l'arme nucléaire. Par cette cyberopération offensive d'une grande complexité, les États-Unis d'Amérique ont démontré leurs capacités dans le domaine cyber et la volonté de s'en servir dans le domaine militaire.

Doctrine des cyberopérations en Israël

Pour Israël, le domaine cyber est un domaine à part entière. L'État est en effet en guerre constante contre des groupes terroristes palestiniens qui n'hésitent pas à attaquer dans le domaine cyber. Pour Israël, la mise en place d'un « Dôme de fer digital » est donc une priorité afin d'assurer sa sécurité dans le cyberespace et empêcher tout impact sur ses forces physiques, constamment engagées.

Les doctrines israéliennes sont cependant non publiques. Néanmoins, il semblerait que ce soient les services de renseignement, en collaboration avec la division information de l'état-major, qui ait la charge de la LID et de la LIO en Israël.[82]

Israël a beaucoup investi dans la recherche et le développement civils dans le domaine cyber. Le gouvernement a également imposé à ses opérateurs vitaux (équivalents des OIV en France) d'allouer plus de 8 % de leur budget à la cybersécurité (contre entre 3 à 4 % en France). Le cyber est donc perçu comme essentiel afin d'assurer la résilience du pays face aux guerres contre le terrorisme et aux menace d'États voisins. L'approche israélienne a fait émerger de nombreuses startups dans le domaine cyber, aujourd'hui à la pointe en termes de technologie.[83]

Israël se distingue des autres pays en termes de doctrine et d'emploi du cyber au vu de son implication dans une guerre quotidienne. Les solutions sont très opérationnelles, en étroite collaboration avec le secteur privé directement financé par l'État. La LID, la LIO et la L2I sont implémentées dans la stratégie globale de cybersécurité et sont complémentaires. L'ambition d'Israël étant de rayonner à l'international dans le domaine cyber, il n'est pas impossible de voir les outils de LID israéliens se répandre à travers le monde, ce qui pourrait en soi impacter dans une certaine mesure la gouvernance du cyberespace à terme, du moins la partie miliaire.

D'un point de vue historique, Israël semble avoir pris part, aux côtés des États-Unis d'Amérique, à la cyberopération visant le programme nucléaire iranien en participant au développement du logiciel malveillant *Stuxnet*.

Israël a également déjà usé de la L2I dans le cadre de l'opération *« Pilier de défense »* en 2012, en utilisant les réseaux sociaux et la diffusion de SMS pour prévenir

la population de l'intervention militaire et dissuader tout acte de résistance. Ils ont également filmé et diffusé en direct l'élimination d'un chef militaire du Hamas. Cependant, une telle utilisation du cyberespace par un État n'est pas sans soulever des questions en termes d'éthique.

3.3.3 Conclusion

Face aux menaces sur le cyberespace et l'intégration du cyber comme un nouveau domaine de lutte à l'image du milieu terrestre, maritime et aérien, les États ont décidé d'agir. Cela se traduit par l'élaboration de stratégies et/ou doctrines sur le domaine afin de définir les enjeux et la politique à mener pour faire face à ces menaces, mais également comment utiliser le domaine cyber à des fins militaires pour appuyer et/ou démultiplier une opération traditionnelle. Le monde civil est intrinsèquement lié à ces stratégies en tant qu'acteur œuvrant pour la cybersécurité des acteurs privés ou bien en développant des solutions de cyberdéfense pour les armées.

Face au terrorisme, la LID participe à la résilience globale d'une Nation. La LIO et la L2I permettent quant à elles de mener le combat contre les terroristes sur le cyberespace afin de ne pas les laisser prospérer sur ce domaine et d'appuyer les éventuelles opérations physiques des forces armées luttant contre les groupes terroristes sur le terrain.

3.4 Conclusion

Rappel de la problématique : Comment s'intègre le cyberespace dans la guerre contre le terrorisme ?

La guerre contre le terrorisme, qu'il soit de nature islamiste à l'image de l'État islamique ou séparatiste à l'image des séparatistes pro-russes dans la guerre du Donbass, prend également place dans le cyberespace. En effet, le cyberespace est désormais le quatrième domaine d'action (après la terre, la mer et l'air). Il n'y a donc pas de cyber-guerre mais des cyberopérations qui viennent appuyer et compléter le champ d'action traditionnel.

Ces cyberopérations sont pour l'heure très tournées vers la guerre par l'information afin de faciliter les opérations militaires vis-à-vis de la population. Cependant, les cyberopérations peuvent avoir une portée plus stratégique avec la réduction des capacités adverses, le renseignement ou bien la réception d'informations pour induire l'ennemi en erreur.

Les États ont bien compris l'importance d'avoir des forces militaires dans le cyberespace et ont élaboré des doctrines et/ou stratégies pour cadrer le développement de ces nouvelles opérations (qu'elles soient défensives, offensives ou d'influence) et unités dédiées. Le monde civil, potentielle cible de cyberattaques par des groupes terroristes, est en général pleinement intégré aux stratégies de cyberdéfense des États.

Nous noterons tout de même que la doctrine française met un point d'honneur au respect du droits international dans la conduite de ses cyberopérations offensives. Ainsi, dans sa doctrine du *Droit international appliqué aux opérations dans le cyberespace*[84], la France remet en cause certaine partie du *manuel de Tallin* et se veut plus protectrice des populations civiles. Cet attachement ne se retrouve pas forcément dans les doctrines ou stratégies de pays étrangers bien qu'ils soient des acteurs majeurs en termes de LID, LIO et L2I.

En conclusion, le cyberespace est devenu un domaine de lutte à part entière dans la guerre contre le terrorisme. Cependant, contrairement aux autres domaines de lutte, la supériorité technologique (cyberarmes) n'est pas la clé pour garantir le succès des opérations militaires contre les groupes terroristes. La lutte contre la propagande et la désinformation semble en effet prédominante à l'heure actuelle ; le défi n'est donc pas uniquement sur le plan technologique, la guerre sur le cyberespace s'accompagne également d'une bonne compréhension psychologique et sociologique des populations visées.

Chapitre 4

Conclusion

L'étude portait sur l'occupation du cyberespace par des groupes terroristes. Cette vaste question a été abordée selon deux aspects. Dans un premier temps, nous avons étudié les formes de l'occupation du cyberespace par des groupes terroristes. Ensuite, l'étude a porté sur la mutation de la guerre contre le terrorisme impliqué par l'utilisation du cyberespace dans cette dernière.

Grâce au premier axe d'étude, nous avons pu conclure que les groupes terroristes sont avant tout des utilisateurs du cyberespace dans le cadre de leurs activités et non une menace pour celui-ci. À l'heure actuelle, ils ne sont également pas une menace pour les populations en menant des cyberattaques.

Le second axe d'étude a mis en évidence l'utilisation du cyberespace dans le cadre de la guerre hybride menée contre des groupes terroristes, notamment au travers de l'exemple ukrainien. Ainsi, dans le cadre de la guerre, le cyberespace devient un domaine de lutte à part entière afin d'appuyer les opérations physiques en cherchant avant tout à impacter les populations.

Afin d'apporter une réponse au sujet de ce mémoire, *L'occupation du cyberespace par des groupes terroristes*, et en reprenant les axes d'étude, nous pouvons établir un tableau représentant le cyberespace selon le modèle des 3 couches et mettre en évidence les formes de l'occupation du cyberespace par des groupes terroristes et les réponses des États face à ces formes d'occupation (Figure 4.1).

Couche	Composition	Principales menaces terroriste	Exemple d'actions menées par des groupes terroriste	Réponses des Etats
Psycho-cognitive	Interprétation, réception et génération des informations par les utilisateurs.	Désinformation, propagande, utilisation du cyberespace à des fins de recrutement,	Désinformation, propagande, recrutement, ciblage d'individus en vue de perpétrer un attentat, communication afin de planifier un attentat.	L2I (contre-propagande, information auprès des populations dans les zones de conflit pour faciliter les opérations militaires), coopération avec les hébergeurs de contenue pour supprimer les publications/sites, en France poursuite judiciaire pour les créateurs de contenue faisant l'apologie du terrorisme.
Logique	Applications, services, protocole et norme composant le cyberespace.	Cyberattaques impactant la disponibilité, l'intégrité et la confidentialité des systèmes d'information.	Cyberattaques peu impactante à base de *script kiddies* (mouvance islamiste), Cyberattaques complexe impactant fortement la disponibilité des systèmes (cybercriminel agissant en parallèle des séparatistes pro-russe).	Domaine couvert par la LID pour l'aspect défensif ainsi LIO pour stopper les services utiliser par les terroristes et/ou source de cyberattaques terroristes.
Physique	Infrastructures réseaux, ordinateurs, entité physique permettant d'accéder au cyberespace.	Destruction des infrastructures impactant l'intégrité et la disponibilité des systèmes d'information.	Pour l'heure, la couche physique n'est pas sujette aux attaques des groupes terroristes.	Domaine couvert par la LID (qui contient un aspect sécurité des équipements physiques) et les mesures de sécurité des infrastructures en général, notamment pour les OIV.

Figure 4.1 : L'occupation du cyberespace par des groupes terroristes et réponses des États selon un modèle en 3 couches

La définition de groupe terroriste reste néanmoins l'objet central de cette étude. La définition ne fait pas l'objet de consensus et cela est d'autant plus vrai dans le cas des guerres hybrides (guerre du Donbass par exemple), où un groupe est jugé comme terroriste selon un belligérant (RPK aux yeux de l'Ukraine) mais légitime aux yeux d'autres pays (la Russie qui y voit la volonté d'un peuple à disposer de lui-même et qui s'implique dans la guerre). Dans le cadre de cette étude, nous nous somme limité au terrorisme islamiste et plus particulièrement à l'État islamique, ainsi qu'au terrorisme séparatiste, notamment dans le cadre du conflit Ukrainien, en abordant la question d'un point de vue ukrainien et occidental. Ces deux cadres limitant l'étude demeurent néanmoins de bons exemples car ils ont été clivants pour les États en matière de guerre et de lutte contre ceux-ci sur le cyberespace.

Enfin, des interviews auraient pu agrémenter l'étude menée sur les signaux faibles afin d'avoir un panel d'avis plus large quant à leur exploitation et pertinence. En effet, bien que la pertinence des signaux faibles soit nuancée, de nombreuse technologies (machine learning, big datas) sont développées afin d'optimiser ces méthodes de veille.

Annexes

Table des annexes

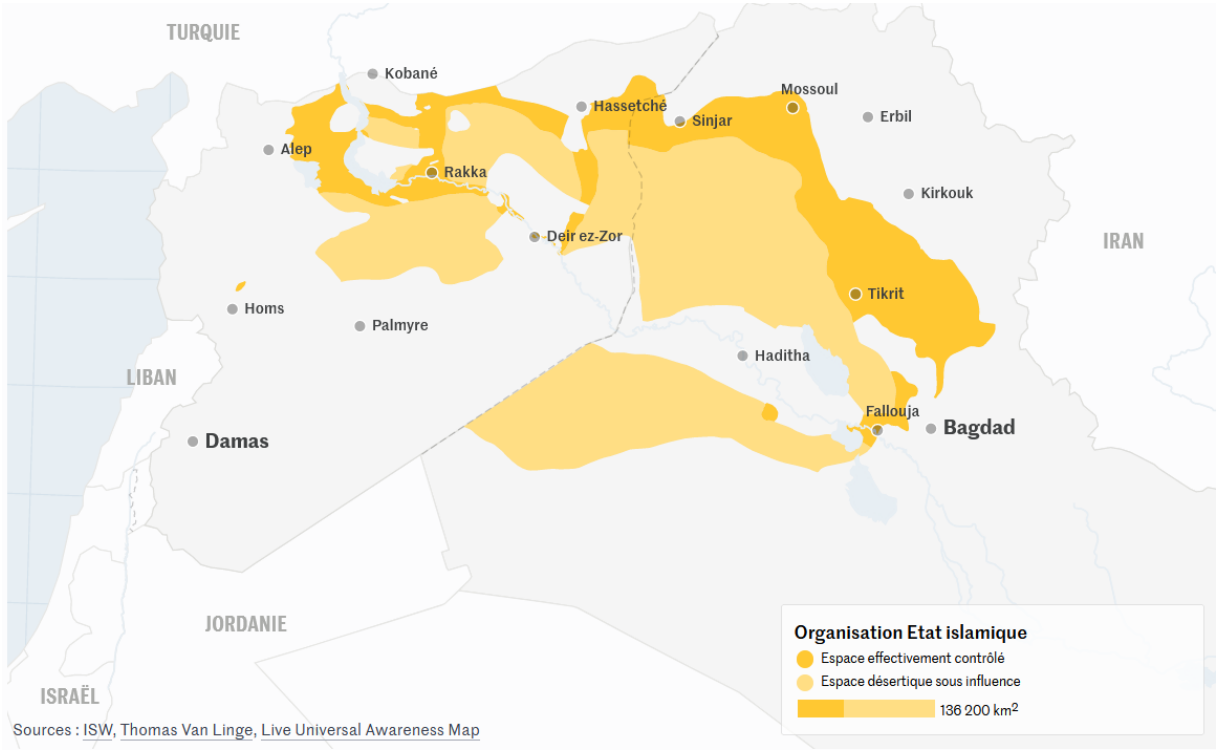
Annexe A

Évolution des territoires de l'État islamique

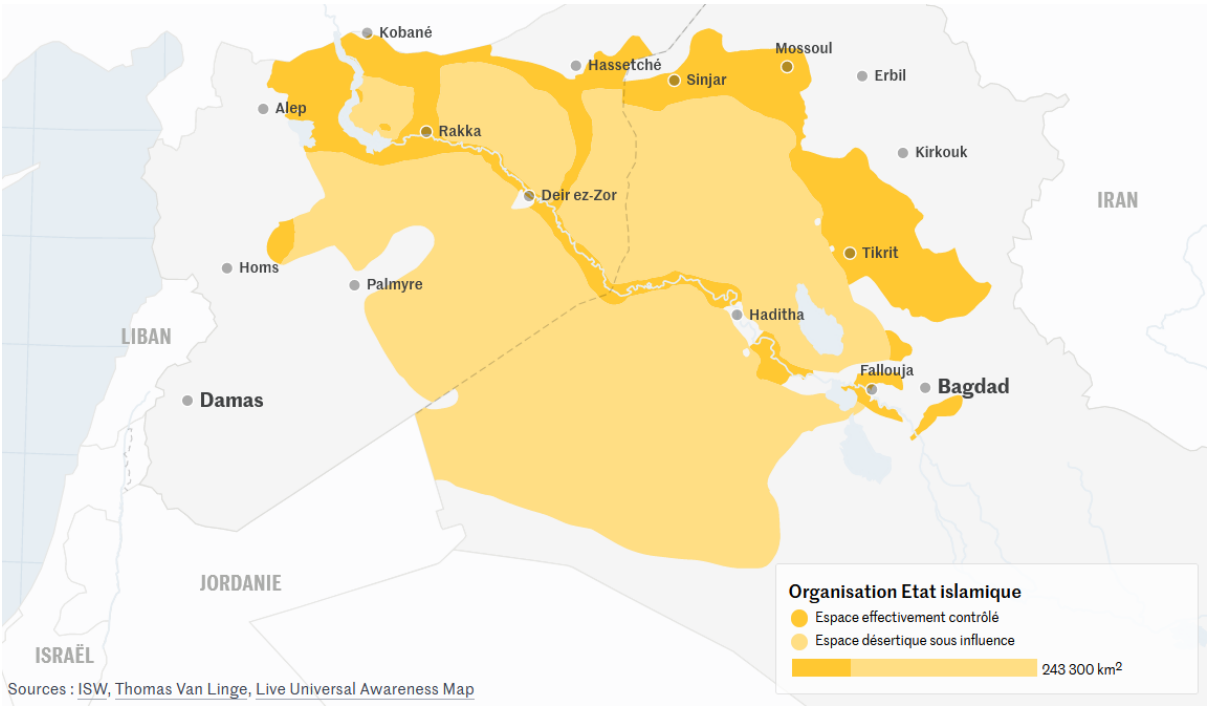
En mars 2019, dans une enquête pour *Le Monde*, le journaliste Pierre Breteau propose 58 cartes afin d'étudier l'évolution du territoire de l'État islamique en Syrie et en Irak. [1] Pour parvenir à ce résultat, le journaliste compile plusieurs sources d'ONG.

Une sélection des cartes clivante permet de comprendre la dynamique de l'évolution des territoires de lÉEtat islamique depuis la proclamation du califat en juin 2014 jusqu'à l'annonce de son élimination par la coalition et les forces démocratiques syriennes.

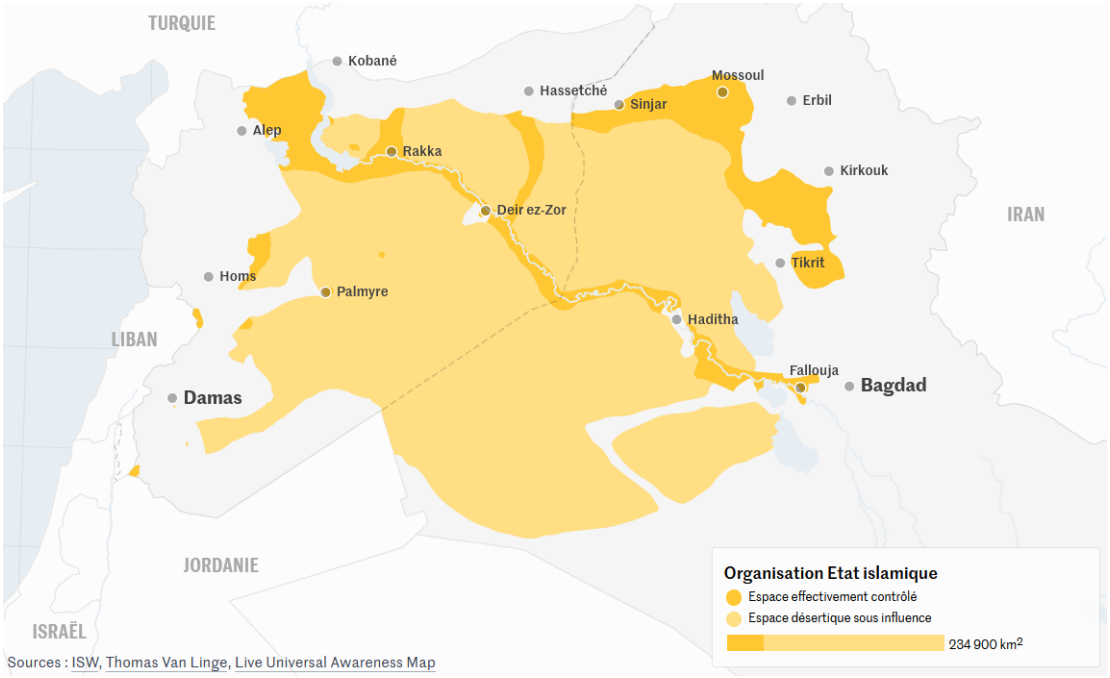
1. BRETEAU Pierre. *Du « califat » à la chute : l'emprise territoriale de l'État islamique en 58 cartes* [en ligne]. Le Monde. 2019. [Consulté le 21 novembre 2020]. Disponible à l'adresse : https ://www.lemonde.fr/les-decodeurs/article/2019/03/26/l-ei-en-58-cartes-de-la-proclamation-du-califat-a-la-fin-de-l-emprise-territoriale_5441495_4355770.html



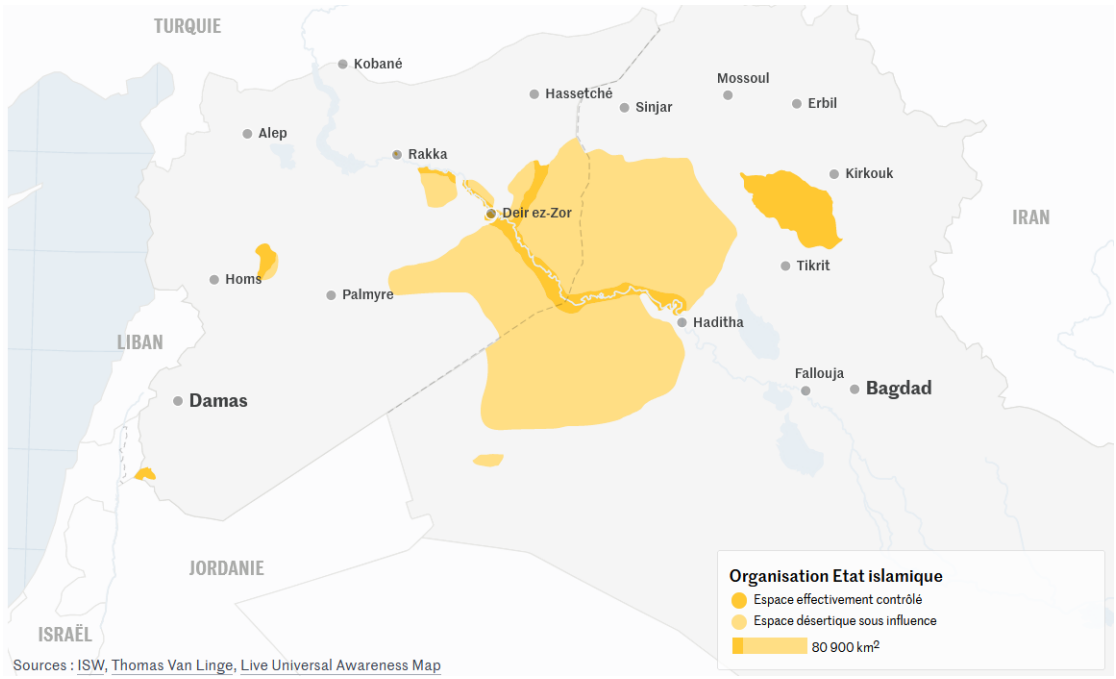
Juin 2014 : Proclamation du califat par l'État islamique.



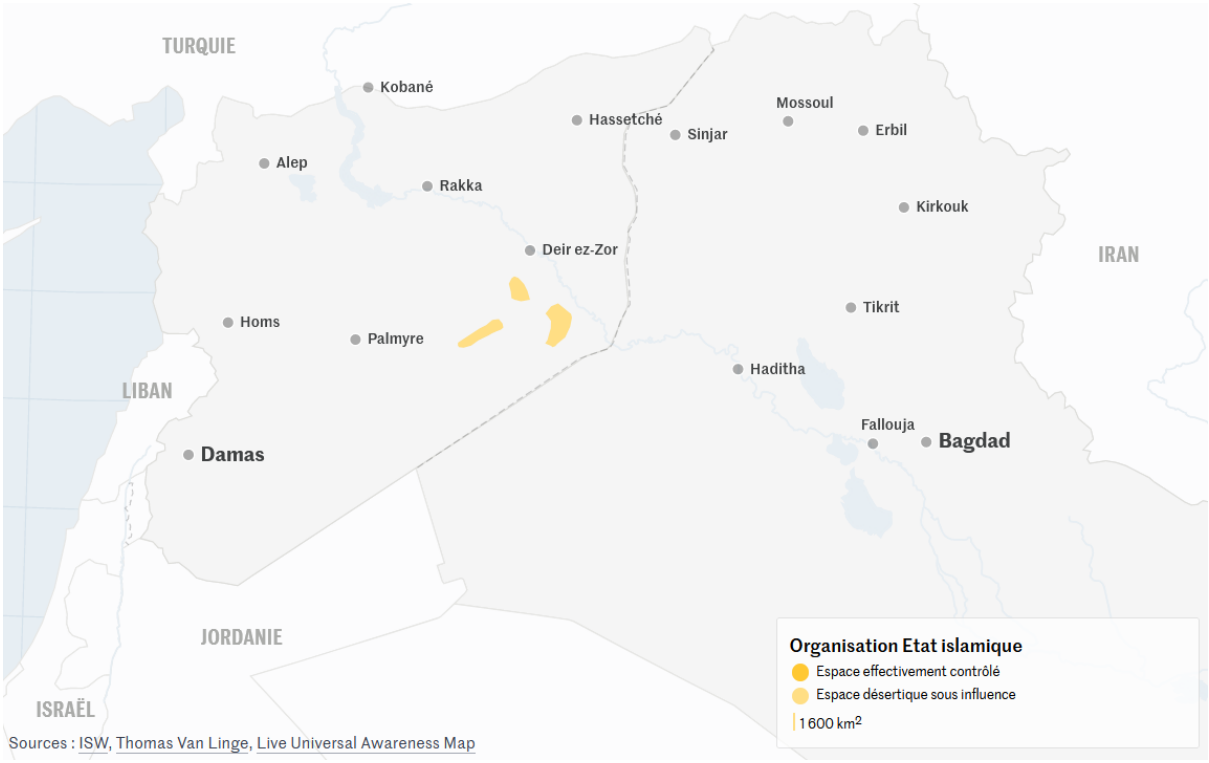
Octobre 2014 : Expansion maximale en Irak et en Syrie.



Janvier 2016 : Durant l'année 2015 l'État islamique à commencer à perdre progressivement des territoires stratégiques après les bombardements français, russe et les succès des armées syriennes et kurdes sur le terrain.



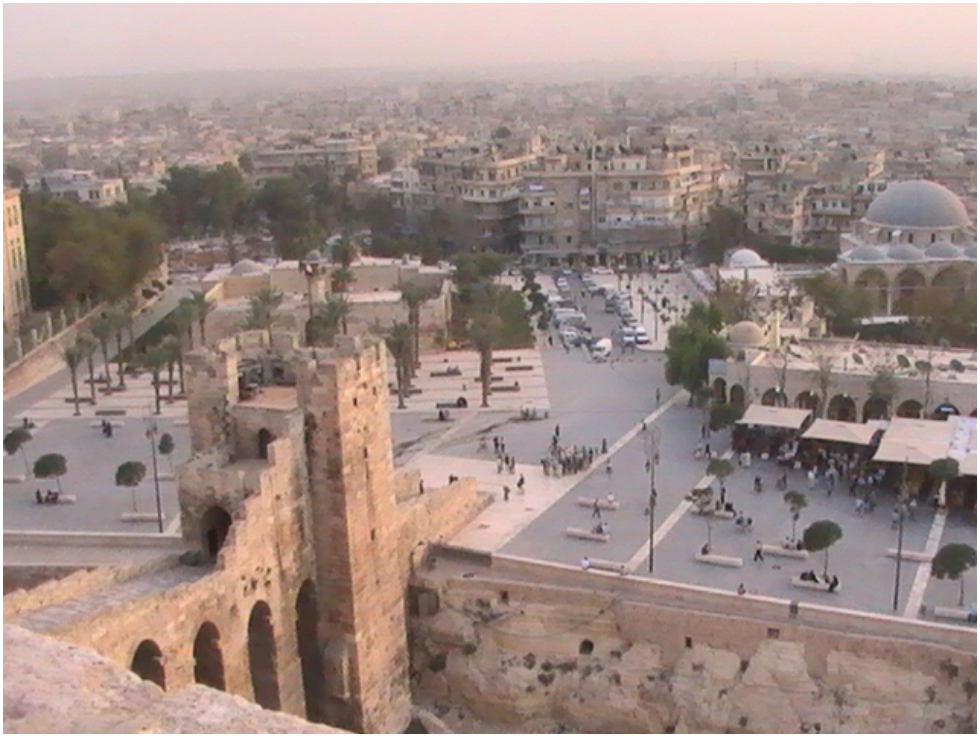
Septembre 2017 : En déclins, l'État islamique perd sa capital, Rakka.



Mars 2019 : l'État islamique n'as quasiment plus de territoire, le groupe est désormais composé de cellule disséminées dans le désert. Le groupe mène désormais une guérilla.

Bien que les villes soient libérées de l'emprise de l'État islamique, les terroristes laissent derrière eux des villes anéantis, bien souvent truffées de pièges mortels. De plus, l'État islamique à détruit une grande partie du patrimoine historique et culturelle dans les territoires qu'il a occupés. Ces lieux culturels et historique ont également été utilisé à des fins macabres à l'image de l'amphithéâtre antique de la ville de Palmyre (Syrie) qui a servis de décor à une vidéo d'exécution de 25 soldats perpétré par des adolescents. [2]

2. EURONEWS. *Syrie : exécution de 25 soldats loyalistes par Daesh à Palmyre* [en ligne]. Euronews. 2015. [Consulté le 21 novembre 2020]. Disponible à l'adresse : https ://fr.euronews.com/2015/07/05/syrie-execution-de-25-soldats-loyalistes-par-daesh-a-palmyre



Ville de Rakka en 2008.
Crédit photo : Amina E.

Ville de Rakka en 2016.
Crédit photo : Directorate-General of Antiquities & Museums

Annexe B

Évolution de l'article 421-2-5-2 du code pénal

Version du 05 juin 2016 au 12 février 2017, créé par la loi n° 2016-731 du 3 juin 2016 - art. 18, abrogée par la décision n° 2016-611 QPC du 10 février 2017.[36]

« Le fait de consulter habituellement un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende.

Le présent article n'est pas applicable lorsque la consultation est effectuée de bonne foi, résulte de l'exercice normal d'une profession ayant pour objet d'informer le public, intervient dans le cadre de recherches scientifiques ou est réalisée afin de servir de preuve en justice. »

Version du 02 mars 2017 au 16 décembre 2017, modifié par la loi n° 2017-258 du 28 février 2017 - art. 24, abrogé par la décision n° 2017-682 QPC du 15 décembre 2017.[37]

« Le fait de consulter habituellement et sans motif légitime un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende lorsque cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ce service.

Constitue notamment un motif légitime tel que défini au premier alinéa la consultation résultant de l'exercice normal d'une profession ayant pour objet d'informer le

public, intervenant dans le cadre de recherches scientifiques ou réalisée afin de servir de preuve en justice ou le fait que cette consultation s'accompagne d'un signalement des contenus de ce service aux autorités publiques compétentes. »

Annexe C

Exemples d'emploi de la LIO au niveau tactique et au niveau stratégique

	Emplois de niveau tactique	Emplois de niveau stratégique
Evaluation des capacités adverses	- Renseignement d'intérêt immédiat lié à l'action des forces	- Renseignement en préparation des opérations, à fins de ciblage ou de développement capacitaire
Réduction voire neutralisation de capacités adverses	- Neutralisation d'un système d'arme - Neutralisation d'un poste de commandement	- Neutralisation d'une capacité opérationnelle adverse (exemple : vecteur de propagande), - Neutralisation d'un système de commandement de niveau stratégique
Action sur les perceptions ou la capacité d'analyse adverse	Altération des données d'un système de commandement	- Désorganisation des centres de propagande adverses

Crédit image : COMCYBER, Éléments publics de doctrine militaire de lutte informatique offensive, 2019

Bibliographie

[1] OLIVIER Sabine. *Terrorisme low cost*. Note du CREOGN Vol. 10, CREOGN. 2015.

[2] BENOIST Hugo. *La guerre à l'heure des réseaux sociaux*. Revue Défense Nationale Vol. 784, pp 53-57. 2015.

[3] LOHARD Audrey. *La genèse inattendue du cyberespace de William Gibson*. Quaderni Vol. 66, pp. 11-13. 2008.

[4] DESFORGES Alix. *Les représentations du cyberespace : un outil géopolitique*. Herodote Vol. 152-153, pp. 67-81. 2014.

[5] LIBICKI Martin. *Conquest in Cyberspace : National Security and Information Warfare*. Cambridge University Press. 2017.

[6] COMCYBER (MINARM). *Eléments publics de doctrine militaire de lutte informatique offensive*. 2019.

[7] VENTRE Daniel. *La cyberguerre des gangs aura-t-elle lieu ?*. Études de l'Ifri, Ifri. 2015

[8] CLAIR-VICTOR Damien. *Qui gouverne l'internet ?*. Université de Technologie de Troyes. 2018

[9] SIZAIRE Vincent. *Quand parler de « terrorisme » ?*. [en ligne]. Le Monde Diplomatique. 2016. [Consulté le 14 octobre 2020]. Disponible à l'adresse : https ://www.monde-diplomatique.fr/2016/08/SIZAIRE/56077

[10] LARANÉ André. *L'État islamique (Daech) entre en action* [en ligne]. Herodote. 2014. [Consulté le 14 octobre 2020]. Disponible à l'adresse : https ://www.herodote.net/5_juin_2014-evenement-20140605.php

[11] PALISSON Miriam. *1er septembre 2004 : la prise d'otages de Beslan par un commando tchétchène*. [en ligne]. France Info. 2015. [Consulté le 03 novembre 2020]. Disponible à l'adresse : https ://www.francetvinfo.fr/monde/russie/1er-septembre-2004-la-prise-d-otages-de-beslan-par-un-commando-tchetchene_3065109.html

[12] JEWISH VIRTUAL LIBRARY. *Vital Statistics : Total Casualties, Arab-Israeli Conflict* [en ligne]. Jewis Virtual Library. 2020. [Consulté le 03 novembre 2020]. Disponible à l'adresse :
https ://www.jewishvirtuallibrary.org/total-casualties-arab-israeli-conflict

[13] HUGHES Matthew, JOHNSON, Gaynor. *Fanaticism and Conflict in the Modern Age*. Chapitre « Religious and nationalist fanaticism ». Édition Routledge. 2004.

[14] VITKINE Benoît. *Terreur sur le Donbass* [en ligne]. Le Monde. 2014. [Consulté le 03 novembre 2020]. Disponible à l'adresse :
https ://www.lemonde.fr/europe/article/2014/07/11/dans-l-est-de-l-ukraine-le-recit-des-survivants-des-geoles-prorusses_4455315_3214.html

[15] DORMAN Veronika. *Donbass : la guerre au fil de l'eau*. Libération. 2019.

[16] DESFORGES Alix. *Cyberterrorisme : quel périmètre ?*. Fiche de l'IRSEM Vol. 11, IRSEM. 2011

[17] KEMPF Olivier. *Le cyberterrorisme : un discours plus qu'une réalité*. Hérodote Vol. 152-153, pp 82-97. 2014

[18] HALLIDAY Josh. *Stuxnet worm is the 'work of a national government agency'* [en ligne]. The guardian. 2010. [Consulté le 03 novembre 2020]. Disponible à l'adresse :
https ://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency

[19] LCI. *Allemagne : premier décès en Europe après une cyberattaque de clinique* [en ligne]. LCI. 2020. [Consulté le 03 novembre 2020]. Disponible à l'adresse :
https ://www.lci.fr/international/allemagne-premier-deces-en-europe-apres-une-cyberattaque-de-clinique-par-des-hackers-2164906.html

[20] BAUMGART Philipe , HASSID Olivier, DELVILLE Thierry, CULLAFFROZ-JOVER Sandrine. *Etat de la menace cyber : COVID-19 et services de santé*. Publication PwC, PwC. 2020

[21] PANTUCCI Raffaello. *A topology of lone wolves : preliminary analysis of lone islamist terrorists*. International centre for the study of radicalisation and political violence. 2011.

[22] GONTAR Patrick, HOMANS Hendrik, ROSTALSKI Michelle, BEHREND Julia, DEHAIS Frédéric, et al.. *Are pilots prepared for a cyber-attack ? A human factorsapproach to the experimental evaluation of pilots' behavior*. Journal of Air Transport Management, Elsevier, vol. 69, pp. 26-37. 2018.

[23] BALDUZZI Marco, WILHOIT Kyle, PASTA Alessandro. *A security evaluation of AIS*. Trend Micro Research Paper, Trend Micro. 2014.

[24] BARICHELLA Arnault. *Cybersécurité des infrastructures énergétiques*. Études de l'Ifri, Ifri. 2018.

[25] HUFFINGTON POST. *A short history of ISIS propaganda videos* [en ligne]. Huffington post. 2018. [Consulté le 19 novembre 2020]. Disponible à l'adresse : https ://www.huffpost.com/entry/isis-propaganda-videos_n_6846688

[26] COMOLI Jean-Louis. *Daech, le cinéma de la mort*. Edition Verdier. 2016.

[27] MATEJIC Nicole. *Guerre de l'information : Daech et son habile maîtrise de la communication* [en ligne]. Nato Review. 2016. [Consulté le 19 novembre 2020]. Disponible à l'adresse : https ://www.nato.int/docu/review/fr/articles/2016/11/16/guerre-de-linformation-daech-et-son-habile-maitrise-de-la-communication/index.html

[28] Guidère Mathieu. *Internet, haut lieu de la radicalisation*. Pouvoirs, Vol. 158 pp 115-123. 2016.

[29] HECKER Marc. *137 nuances de terrorisme. Les djihadistes de France face à la justice*. Études de l'Ifri, Ifri. 2018.

[30] GOZLAN Angélique. *L'adolescence face à la propagande visuelle 2.0 de Daesh*. Cahiers de psychologie clinique, Vol. 49 pp 211-226. 2017.

[31] Bouzar DOUNIA, CAUPENNE Christophe, VALSAN Sulayman. *La metamorphose opérée chez le jeune par les nouveaux discours terroristes*. Centre de prévention des dérives sectaires liées à l'Islam. 2014.

[32] HARBULOT Christian. *La France peut-elle vaincre Daech sur le terrain de la guerre de l'information ?*. Ecole de guerre économique. 2015.

[33] 20 Minutes. *Un combattant de Daesh appelle ses «frères» à de nouvelles actions en France* [en ligne]. 20 Minutes. 2015. [Consulté le 19 novembre 2020]. Disponible à l'adresse : https ://www.20minutes.fr/monde/1537631-20150210-combattant-daesh-appelle-freres-nouvelles-actions-france

[34] AUTET Marie-Alix, LAEMLE Brice. *Un site officiel contre le cyberdjihadisme* [en ligne]. France Culture. 2015. [Consulté le 19 novembre 2020]. Disponible à l'adresse : https ://www.franceculture.fr/numerique/un-site-officiel-contre-le-cyberdjihadisme

[35] GOUVERNEMENT FR. *#Stopdjihadisme : Ils te disent...* [vidéo en ligne]. Dailymotion, 1min55. 2015. [Consulté le 19 novembre 2020]. Disponible à l'adresse : https ://www.dailymotion.com/video/x2fpywn

[36] PRESIDENT DE LA REPUBLIQUE. *LOI no 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme*. Journal officiel n° 0263 du 14/11/2014. 2014.

[37] PRESIDENT DE LA REPUBLIQUE. *LOI no 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale*. Journal officiel n° 0129 du 04/06/2016. 2016.

[38] CONSEIL CONSTITUTIONEL. *Décision no 2016-611 QPC du 10 février 2017*. Journal officiel n° 0037 du 12/02/2017. 2017.

[39] CONSEIL CONSTITUTIONEL. *Décision no 2017-682 QPC du 15 décembre 2017*. Journal officiel n° 0293 du 16/12/2017. 2017.

[40] ANSOFF Igor, MCDONNELL Edward J.. *Implanting Strategic Management*. Prentice Hall. 1990.

[41] DONADINI Anne. *Qui sont les partisans de Daech sur internet ?* [en ligne]. Les Inrockuptibles. 2015. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https ://www.lesinrocks.com/2015/03/24/web/actualite/dou-viennent-les-tweets-des-djihadistes-de-daech/

[42] HARBULOT Christian. *La France peut-elle vaincre Daech sur le terrain de la guerre de l'information ?*. Ecole de guerre économique. 2015.

[43] BERGER J.M.. *How ISIS Games Twitte* [en ligne]. The Atlantic. 2014. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https ://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

[44] RENAULT Laurène. *Sur les réseaux sociaux, une djihadosphère en constante évolution* [en ligne]. The Conversation. 2020. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https ://theconversation.com/sur-les-reseaux-sociaux-une-djihadosphere-en-constante-evolution-149754

[45] MEMRI. *Le nouveau chant en français de l'EI « Ma vengeance » justifie le terrorisme en Europe et fait l'éloge des attentats de Paris et de Bruxelles* [en ligne]. MEMRI FR. 2016. [Consulté le 30 novembre 2020]. Disponible à l'adresse : http ://memri.fr/2016/07/07/le-nouveau-chant-en-francais-de-lei-ma-vengeance-justifie-le-terrorisme-en-europe-et-fait-leloge-des-attentats-de-paris-et-de-bruxelles/

[46] LAURENT Samuel. *Terrorisme : qu'est-ce que la fiche « S » ?* [en ligne]. Le Monde. 2015. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https ://www.lemonde.fr/les-decodeurs/article/2015/08/31/terrorisme-peut-on-sanctionner-les-personnes-faisant-l-objet-d-une-fiche-s_4741574_4355770.html

[47] SAFFRON. *Projet SAFFRON* [en ligne]. SAFFRON. 2016. [Consulté le 30 novembre 2020]. Disponible à l'adresse : http ://www.saffron-project.eu/fr/projet/

[48] ALLOING Camille, MOINET Nicolas. *Les signaux faibles : du mythe à la mystification*. Hermès Vol. 76, pp. 68-76. 2016.

[49] SCHITTLY Richard. *Dans le contexte terroriste, plus d'incidents et de fausses alertes* [en ligne]. Le Monde. 2016. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https ://www.lemonde.fr/police-justice/article/2016/08/09/le-contexte-terroriste-suscite-de-droles-de-passages-a-l-acte_4980086_1653578.html

[50] SOTTEK T.C., KOPFSTEIN Janus. *Everything you need to know about PRISM* [en ligne]. Le Monde. 2013. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https ://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

[51] GUENET Florian. *Samuel Paty : des sites français visés par des cyberattaques avec des messages violents* [en ligne]. La nouvelle tribune. 2020. [Consulté le 30 novembre 2020]. Disponible à l'adresse : https ://lanouvelletribune.info/2020/10/samuel-paty-des-sites-francais-vises-par-des-cyberattaques-avec-des-messages-violents

[52] MATTIS James N., HOFFMAN Frank. *Future Warfare : The Rise of Hybrid Wars*. USNI. Publication of USNI Vol. 132/11/1,233. 2005.

[53] KROLIKOWSKI Hubert. *L'origine et les caractéristiques de la guerre irrégulière*. Stratégique Vol. 100/101, pp. 13-28. 2012.

[54] VAN PUYVELDE Damien. *La guerre hybride existe-t-elle vraiment ?* [en ligne]. NATO Review. 2015. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https ://www.nato.int/docu/review/fr/articles/2015/05/07/la-guerre-hybride-existe-t-elle-vraiment/index.html

[55] TENENBAUM Elie. *Le piège de la guerre hybride*. Études de l'Ifri, Ifri. 2015

[56] JASPER Scott, MORELAND Scott. *The Islamic State is a Hybrid Threat : Why Does That Matter ?* [en ligne]. Small Wars Journal. 2014. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https ://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter

[57] DE CARLO DEVIC Alexandre. *La Guerre au XXIe siècle : La Guerre hybride, nouvel outil stratégique du Kremlin* [en ligne]. La revue d'histoire militaire. 2020. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https ://larevuedhistoiremilitaire.fr/2020/05/06/guerre-hybride-nouvel-outil-strategique-kremlin/

[58] KEMPF Olivier. *Ducyber et de la guerre*. Fondation pour la Recherche Stratégique. 2019.

[59] NOISETTE Thierry. *Pour l'armée, le cyber devient un champ de bataille à part entière* [en ligne]. L'OBS. 2017. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https ://www.nouvelobs.com/rue89/rue89-nos-vies-connectees/20161221.RUE6049/pour-l-armee-le-cyber-devient-un-champ-de-bataille-a-part-entiere.html

[60] CARTWRIGHT James E.. *Joint Terminology for Cyberspace Operations*. Département de la défense américain. 2017.

[61] CORNISH P., LIVINGSTONE D., CLEMENTE D., YORKE C.. *On cyber warfare*. Chatham House Report. 2010.

[62] SCHMITT Michael N.. *Tallinn Manual on the International Law Applicable to Cyber warafare*. Cambridge university press. 2013.

[63] ROMANI Roger. *Rapport d'information au nom de la commission des Affaires étrangères, de la défense et des forces armées sur la cyberdéfense*. Sénat, session extraordinaire. 2008.

[64] RID Thomas. *Cyber war will not take place*. King's College London. 2011.

[65] DELERUE François. *Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations*. Étude prospective et stratégique. 2017.

[66] HARBULOT Christian. *Le monde du renseignement face à la guerre de l'information*. Hermès Vol. 76, pp. 80-85. 2016.

[67] PETIT Romain. *Qu'est-ce que la guerre psychologique ? (3/3)* [en ligne]. Opérationnels. 2019. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https ://operationnels.com/2019/08/27/quest-ce-que-la-guerre-psychologique-3-3-2/

[68] ROGEL Bernard. *Vers une approche globale de la gestion des conflits*. Armées d'aujourd'hui Vol. 360, pp 48-59. 2011.

[69] LAGNEAU Laurent. *Sahel : Sur les réseaux sociaux, la force Barkhane est visée par une campagne de fausses informations* [en ligne]. opex360. 2019. [Consulté le 12 décembre 2020]. Disponible à l'adresse : http ://www.opex360.com/2019/12/05/sahel-sur-les-reseaux-sociaux-la-force-barkhane-est-visee-par-une-campagne-de-fausses-informations/

[70] DUGOIN-CLEMENT Christine. *La guerre hybride en Ukraine*. Revue Défense Nationale Vol. 793, pp 85-90. 2016.

[71] DE LA VILLARDIERE Bernard. *Russie : la nouvelle guerre froide*. Enquête exclusive, 1h15min. 2020.

[72] COURRIER INTERNATIONAL. *Petya, un virus qui a paralysé l'Ukraine avant de frapper ailleurs* [en ligne]. Courrier international. 2017. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https ://www.courrierinternational.com/article/cybersecurite-petya-un-virus-qui-paralyse-lukraine-avant-de-frapper-ailleurs

[73] DURAND Corentin. *L'armée séparatiste pro-russe bombarde les Ukrainiens de propagande par SMS* [en ligne]. Numerama. 2017. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https ://www.numerama.com/politique/257663-larmee-separatiste-pro-russe-bombarde-les-ukrainiens-de-propagande-par-sms.html

[74] GREENBERG Andy. *How an Entire Nation Became Russia's Test Lab for Cyberwar* [en ligne]. Wired. 2017. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https ://www.wired.com/story/russian-hackers-attack-ukraine/

[75] ANSSI. *Défense et sécurité des systèmes d'information, Stratégie de la France*. 2011.

[76] COMCYBER (MINARM). *Politique ministérielle de lutte informatique defensive*. 2019.

[77] ASSEMBLEE NATIONALE. *Compte rendu, Commission de la défense nationale et des forces armées, Audition du général de division aérienne Didier Tisseyre, général commandant la cyber défense sur le thème « le cyber, nouvel espace de conflictualité »*. 2020.

[78] LES ECHOS. *La Russie adopte une "doctrine" de cybersécurité* [en ligne]. Les échos. 2016. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https ://www.lesechos.fr/2016/12/la-russie-adopte-une-doctrine-de-cybersecurite-221397

[79] LITOVKINET Nikolaï. *Que contient la nouvelle doctrine de cybersécurité russe ?* [en ligne]. Russia Beyond. 2016. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https ://fr.rbth.com/ps/2016/12/07/que-contient-la-nouvelle-doctrine-de-cybersecurite-russe_654461

[80] BUREAU DU PRESIDENT DES USA. *National Cyber Strategy*. 2018.

[81] BOCKEL Jean-Marie. *La cyberdéfense : un enjeu mondial, une priorité nationale*. Rapport d'information du Sénat Vol. 681. 2020.

[82] RAZOUX Pierre. *La pensée stratégique israélienne confrontée à la nouvelle donne au Moyen-Orient*. IRSEM, Note de recherche stratégique 7. 2014.

[83] CIGREF. *Cyber & innovation en Israël*. Cigref, publication du Cigref. 2019.

[84] MINARM. *Droit international appliqué aux opérations dans le cyberespace*. Délégation à l'information et à la communication de la défense. 2019.