Instrumentalisation du cyberespace :

Les outils numériques comme armes de déstabilisation

Emma Gueguen

Werra

Février 2022

Après deux ans de classe préparatoire littéraire et une L3 en Relations Internationales à l'ISIT, **Emma Gueguen** a intégré cette année le Master 2 - Stratégies Internationales et Diplomatie à l'ISIT. Elle rédige actuellement son mémoire sur les stratégies d'influence des entreprises chinoises de télécommunication en Europe, avec une étude de cas sur Huawei. Passionnée par l'intelligence économique, elle effectue une alternance en compliance LCB-FT (*Lutte contre le blanchiment et le financement du terrorisme*).

INTRODUCTION

Le 26 janvier 2021 avait lieu le Panorama annuel de la cybercriminalité du Clusif (Club de la sécurité de l'information français). À cette occasion, Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), a déclaré au sujet de l'état des menaces cyber, que « l'heure [était] grave »[1]. Un an plus tard, cette affirmation est toujours d'actualité. Pouvant être défini comme un espace d'interconnexion et de communication entre les différents réseaux et à l'échelle mondiale, le cyberespace n'est délimité par aucune frontière visible et les enjeux stratégiques qui en découlent ne sont pas toujours encadrés juridiquement. Depuis plus d'une dizaine d'années maintenant, les technologies et les outils numériques (que l'on peut définir comme étant l'ensemble des outils qui fournissent des données numériques et fonctionnent grâce à elles, comme les téléphones, les ordinateurs, les objets connectés, le cloud, etc.) ne cessent d'évoluer : du simple nouveau modèle de téléphone à une numérisation intensive de certaines activités, le monde est de plus en plus connecté.

À l'ère de l'explosion du numérique, les informations et les données sont devenues des facteurs clés pour les acteurs, et c'est autour d'elles que s'organisent les attaques pour tenter de les récupérer ou de les compromettre, mais que s'organise aussi la protection des infrastructures et des systèmes. Bien que les attaques immatérielles à l'encontre d'individus ou d'acteurs majeurs (États, grandes entreprises, etc.) aient toujours existé, elles se sont maintenant démultipliées et généralisées. Ces attaques, d'un simple mail de *phishing* à un rançongiciel ou à une cyberattaque généralisée sur un service étatique par exemple, sont le symbole d'une hyperconnexion qui n'est pas sans risque, et synonymes d'un nouveau type de guerre entre les acteurs. En effet, pour les États comme les entreprises, la question de la souveraineté et de l'influence n'est pas anodine : en cas de tensions et afin d'éviter des affrontements directs, les attaques (cyberattaques, batailles d'influence ou propagande sur les réseaux sociaux, etc.) visant à atteindre la souveraineté numérique et nationale d'un acteur sont désormais très souvent dématérialisées. Le cyberespace est donc devenu un lieu plus que propice pour ces offensives, et pourrait être qualifié de nouveau champ de bataille, dont le manque de frontières permet une plus grande liberté dans la façon qu'ont les acteurs de s'affronter.

[1] Juliette Paoli, « Cybermenaces : « L'heure est grave », Guillaume Poupard », *www.solutions-numériques.com*, 26 janvier 2021, consulté le 20.01.22, lien.

L'objet de cet article sera de comprendre comment les outils numériques peuvent être utilisés à des fins de déstabilisation par certains acteurs dans leur lutte pour la souveraineté, et la façon dont le cyberespace est instrumentalisé pour y parvenir.

Acteurs du numérique et instrumentalisation progressive du cyberespace : L'apparition de nouveaux enjeux géopolitiques

1. L'évolution du cyberespace et des outils numériques

Selon l'ANSSI, le cyberespace est « *l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérisées* »[2]. En fonction des auteurs, il est décrit comme étant constitué de 3, 5 ou 7 couches. Dans le cadre de cet article, nous parlerons de 3 couches. La première est la couche "physique" ou "matérielle", qui regroupe les infrastructures de réseau : câbles, ordinateurs, serveurs, etc. Elle permet le fonctionnement d'internet et des réseaux et est inscrite sur un territoire, ce qui en fait une couche soumise à une législation nationale. La seconde, dite "logique", est formée par une architecture contenant les codes et les programmations qui permettent aux machines de faire circuler les informations et de communiquer entre elles au sein d'un réseau. La dernière couche "sémantique" ou "cognitive", comporte les données qui sont diffusées et transportées *via* les réseaux et qui contiennent des informations sur les utilisateurs. Ces trois couches découlent de la création de l'Arpanet en 1969, modèle en réseau qui inspire la création du World Wide Web et 1990, et le développement de l'ICANN dès 1998, qui attribue des noms de domaines et des identifiants Internet, permettent un accroissement rapide des communications et de l'échange d'informations. Elles sont à prendre en compte lorsqu'on appréhende le cyberespace dans sa totalité. Ce dernier est notamment utilisé *via* des outils numériques en tout genre (ordinateurs, téléphones, objets connectés, etc.), dont l'accroissement et le développement technologique ont été fulgurants ces quinze dernières années. L'évolution des outils numériques est marquée par trois tournants différents : les années 1980, avec la naissance d'Internet et de l'ordinateur personnel ; les années 1990 avec une croissance exponentielle de l'utilisation d'Internet ; et les

[2] ANSSI, glossaire "cyberespace", consulté le 20.01.22 lien

années 2000/2010, avec les smartphones, les objets connectés et le développement de plus en plus poussé de l'intelligence artificielle.

Ces évolutions ont permis la construction d'un espace qui a démultiplié les échanges et les possibilités de communication grâce à l'échange d'informations et la multiplication de contenus en tout genre. La numérisation de l'information et de nombreux secteurs a totalement changé la façon dont nous vivons : nouveaux moyens de paiement, carte de transports sur notre téléphone, etc. Les outils numériques nous facilitent la vie, mais l'exposent également plus aux risques qui accompagnent cette numérisation, dus à de nouveaux types de vulnérabilité. Les informations sont devenues très valorisables, et cela a conduit à une compétition des acteurs sur l'espace cyber, qui a elle-même progressivement mené à des confrontations de plus en plus importantes. Cette conflictualité omniprésente est apparue progressivement. Cela a par conséquent amené un changement de paradigme dans la façon dont le cyberspace est utilisé : à l'origine un espace de commandement et de communication, il est devenu un espace de stockage et d'échange d'informations qui sont de plus en plus utilisées à des fins géopolitiques. C'est donc un espace qui s'est vu être militarisé dans une lutte pour la souveraineté numérique par différents acteurs, ce qui a mené à l'apparition de nouveaux enjeux stratégiques.

2. Cyberespace et enjeux géopolitiques nouveaux : disparition des frontières et territoires interconnectés

Ces différents acteurs (États, grandes entreprises, associations, particuliers) ont vu dans le cyberespace un nouveau moyen de s'affronter. Là où les conflits se faisaient sur un espace physique véritable et donnaient lieu à des pertes plus graves (en moyens financiers, matériels et humains), l'utilisation du cyberespace permet un nouveau type d'affrontement. En effet, l'élément principal qui caractérise cet espace est qu'il est dématérialisé : cela signifie qu'il ne possède pas de frontières véritables et que le transfert d'informations peut se faire aux quatres coins du globe. Cette absence de frontières redéfinit toute la notion de conflit entre les acteurs et soulève de nouveaux enjeux géopolitiques : alors que la géopolitique étudie les rivalités de pouvoir[3] et les conflits sur un territoire donné, qui est lui-même défini par des frontières, le cyberespace pose le problème de la définition de sa délimitation et de des limites de sa souveraineté. Dès lors, l'hyperconnexion, l'accès à tout l'espace numérique et à un grand nombre de données permettent aux acteurs de s'installer sur un espace offrant un champ de possibilités beaucoup plus vaste qu'un espace physique pour tenter de déstabiliser un

[3] Frédérick Douzet, "La géopolitique pour comprendre le cyberespace", *Hérodote*, 2014, consulté le 20.01.22 lien

adversaire. Leur puissance en est donc bouleversée : là où il était principalement question des moyens militaires et sécuritaires d'un État pour établir son niveau d'influence et de puissance, il faut désormais ajouter la souveraineté numérique à cette combinaison.

3. Le numérique : utilisation généralisée et instrumentalisation progressive

Les outils numériques d'aujourd'hui comme le téléphone, l'ordinateur portable, les objets connectés, n'étaient pas des objets ayant normalement pour but d'être utilisés à des fins d'affrontement ou d'espionnage. Il n'est pas anormal, dans un monde en connexion constante, de posséder des outils qui permettent de communiquer et de diffuser des informations. Le passage aux smartphones et aux outils connectés a généralisé leur utilisation, qui va de pair avec leur instrumentalisation. Via ces derniers se trouve l'accès universel à Internet. Ce dernier a donné lieu à une diffusion massive et à une multiplication des données, laissées à la libre disposition de différents acteurs : entreprises privées, États, GAFAM, BATX. La récolte d'informations à des fins de déstabilisation ou d'opérations d'influence en devient un élément lié incontournable : pour ne donner qu'un exemple concret, il est possible de citer le scandale lié à l'entreprise Cambridge Analytica en mars 2018. L'entreprise Facebook (aujourd'hui Meta), qui compte des milliards d'utilisateurs, a été accusée d'avoir permis la récolte de données de près de 87 millions d'utilisateurs par Cambridge Analytica, lesquelles ont ensuite été utilisées par l'équipe de campagne de Donald Trump lors de l'élection présidentielle américaine de 2016, afin de « changer la perception du public »[4]. Là où Facebook est un réseau social qu'un individu lambda va utiliser pour le loisir, les informations qu'il ajoute et partage pourront être utilisées (parfois contre son gré) par d'autres acteurs.

Ce cas n'est néanmoins qu'un exemple parmi tant d'autres. L'évolution des services proposés par des outils numériques et du cyberespace est importante, et leur instrumentalisation peut être intensifiée bien au-delà de "simples" luttes d'influence, tandis que l'accroissement des affrontements à l'aide du cyber est visible depuis plusieurs années : cyberespionnage, attaques informatiques, propagande informationnelle…

Le passage d'un monde mondialisé à un monde hyperconnecté et en évolution constante grâce au développement du cyberespace a mené au bouleversement des rapports de force entre les acteurs : ces derniers voient leur souveraineté numérique être constamment menacée. Quels

[4] Damien Leloup et Martin Untersinger, entretien avec Christopher Wylie, « Cambridge Analytica a fermé mais ses pratiques n'ont pas disparu », *Le Monde*, 11 mars 2020, consulté le 21.01.22 lien

sont les motifs qui justifient ce changement de paradigme ? Comment le cyberespace permet-il ces nouveaux affrontements ?

L'utilisation des outils numériques comme arme de déstabilisation

1. Motivations et objectifs

Quels sont les intérêts d'utiliser le cyberespace et les outils numériques pour tenter de déstabiliser un adversaire ou un concurrent ? Dans le cadre d'une guerre, « maîtriser l'information tant sur le plan stratégique qu'opérationnel »[5] est essentiel : dans le cyberespace et dans un monde de plus en plus connecté, cette maîtrise de l'information est la clé qui peut permettre la réussite. Le cyberespace apporte des nouveautés dans la manière de faire la guerre. Déstabiliser son adversaire peut se faire par une guerre de l'influence : les motivations pour influencer l'opinion publique sont nombreuses (élections présidentielles, concurrence sur le marché dans un secteur particulier, etc.). Ainsi, la maîtrise et la manipulation des données trouvables sur le cyberespace permettent de modifier l'opinion d'un individu sur un sujet donné. Dans son article, Solange Chernaouti-Hélie fait référence au concept d'*information as a weapon*[6] : propagande, *fake news*, fuites de documents sur un sujet ou sur un individu… Les capacités de communication *via* Internet permettent un accès généralisé à l'information, mais aussi à sa manipulation. En cela, le cyberespace devient un outil plus qu'efficace lors de conflits et d'affrontements entre des acteurs : l'auteur explique ainsi qu'il faut désormais « considérer les technologies de l'information et de la communication comme des innovations dans l'art de faire la guerre. Internet, les ordinateurs, le code informatique ainsi que les données, sont de nouvelles armes de guerre dans un nouveau champ de bataille qu'est le cyberespace ».

Au-delà des capacités d'influence et de manipulation qu'apporte le cyberespace, s'affronter sur une zone dématérialisée contient aussi plusieurs avantages. En effet, à la différence d'attaques physiques, les cibles visées sont des serveurs, des réseaux, des systèmes informatiques, qui contiennent des informations, qui sont très importants ou vitaux pour ceux qui les possèdent, et qui sont atteignables *via* d'autres outils numériques ; et en cela, ces attaques n'impliquent pas de pertes humaines. Ces attaques et ces méthodes ne demandent par ailleurs

[5] Solange Ghernaouti-Hélie, « Menaces, conflits dans le cyberespace et cyberpouvoir », *Sécurité et Stratégie*, mars 2011, lien, consulté le 21.01.22
[6] *Ibid.*

pas autant de matériel qu'en véritable en zone de conflit : cela permet de les rendre plus précises et plus rapides, voire plus efficaces. Non seulement ces dernières sont généralement moins coûteuses, mais elles garantissent un certain niveau d'anonymat, bien qu'il soit parfois possible de déduire ou de découvrir l'origine de l'attaque.

Le cyberespace et les outils numériques ont beaucoup de failles, notamment à cause de l'hyperconnexion et des nouvelles évolutions du secteur. Ils n'avaient à l'origine pas vocation à être utilisés respectivement comme zone et armes de déstabilisation, mais cette instrumentalisation est apparue avec la multiplication des flux de données et de communication. Dès lors, peu d'acteurs avaient conscience qu'il fallait apprendre à se défendre face aux possibles attaques, et encore aujourd'hui, ce manque de défense est une grosse opportunité pour ceux qui se servent du cyber et du numérique pour attaquer.

2. Les moyens

L'objectif de cet article n'est pas de donner une liste exhaustive ou de dresser une typologie des attaques ou des méthodes de déstabilisation qui peuvent être utilisées dans le cyberespace, mais d'en citer certaines pour illustrer des exemples de tentatives de déstabilisation *via* l'utilisation du cyberespace. La multitude de ressources pour ce faire permet à l'utilisateur de déstabiliser sa cible de la manière de son choix et de la façon la plus précise possible.

L'une des premières utilisations faite du cyberespace et des outils numériques est celle du cyberespionnage, à plusieurs degrés : d'un "simple" piratage d'un compte Messenger, à des attaques plus poussées pour obtenir des renseignements stratégiques. Un exemple parlant est celui des groupes APT (*Advanced Persistent Threat*), qui sont très souvent financés et soutenus par des États : ils sont donc très structurés et possèdent beaucoup de moyens pour mener à bien leurs attaques. Ces groupes développent des attaques d'un niveau technique élevé, et travaillent durant plusieurs mois ou plusieurs années afin d'obtenir des données ou d'attaquer les infrastructures et serveurs, grâce aux vulnérabilités et aux failles découvertes chez la cible. Le groupe *APT31* est affilié à l'État chinois et a fait l'objet d'un rapport de l'ANSSI[7] le 15 décembre 2021, après une campagne d'attaques sur des entités françaises à l'aide d'un « code malveillant baptisé Pakdoor par l'ANSSI ». Ce rapport permet d'observer de manière détaillée la façon dont le groupe APT a pénétré les infrastructures et les serveurs des entités françaises,

[7] ANSSI, « Campagne d'attaque du mode opératoire APT31 : description, contre-mesures et code », dans le cadre d'une vaste campagne d'attaques à l'encontre d'entités françaises liée au mode opératoire d'attaque (MOA) APT31, 15 décembre 2021, consulté le 29.01.22, lien

en exploitant les vulnérabilités et en contournant les protections numériques des victimes. Cela leur a notamment permis d'obtenir des données telles que les « bases de données d'utilisateurs, des courriels et des données métiers sensibles »[8]. Au-delà de la collecte de données, ces groupes peuvent aussi avoir pour objectif d'arrêter le fonctionnement d'un système ou de l'endommager.

L'obtention d'informations via la collecte de données volées ne se fait pas seulement grâce à des groupes comme *APT31* ou *APT28* (Russie), mais aussi grâce à des logiciels espions. L'un des plus connus à date est le logiciel israélien Pegasus, qui a été mis en lumière courant juillet 2018 après qu'un consortium de médias ait révélé qu'il avait potentiellement ciblé plus de 50 000 numéros de téléphones[9], pour le compte de plusieurs États. Parmi les numéros : militants, personnes politiques haut-placées, journalistes, opposants politiques, avocats… La façon dont les données collectées sont utilisées n'est pas précisée, mais il est évident que leur collecte et donc leur utilisation sont illégales, puisque le logiciel est implanté à l'insu de la cible. Dans un communiqué officiel, le Ministère des Affaires Étrangères finlandais déclarait le 28 janvier 2022 que certains diplomates finlandais avaient été victimes d'espionnage par le logiciel développé par NSO Group.[10]

L'un des types d'attaques les plus communs et dont le nombre a explosé en 2021 est le rançongiciel (ou *ransomware* en anglais) : l'individu ou le groupe effectuant l'attaque (particulier comme groupe spécialisé, sur "commande" ou décision individuelle) placent sur l'outil numérique visé (ordinateur, téléphone…) un logiciel malveillant, un *malware*, qui va verrouiller et chiffrer des fichiers ou toutes les données de l'appareil, en échange d'une rançon. Selon le Département du Trésor des États-Unis, le montant des rançons des rançongiciels aurait été de 590 millions de dollars dans la première moitié de 2021, contre 416 millions de dollars en 2020[11].

Le cyberespace offre une immense variété de contenus, qu'ils aient été obtenus légalement ou non. L'accès à l'information permet d'appuyer, ou au contraire, de réduire l'influence d'un acteur, et donc d'affecter sa réputation. Dès lors, l'un des meilleurs moyens

---

[8] *Ibid.*

[9] Damien Leloup et Martin Untersinger, « « Projet Pegasus » : révélations sur un système mondial d'espionnage de téléphones », *Le Monde*, 18 juillet 2021, consulté le 29.01.22, lien

[10] Ministère des Affaires Étrangères de Finlande, « Ministry for Foreign Affairs has solved suspected espionage case », dans le cadre de l'espionnage d'un Ministre finlandais grâce au logiciel espion Pegasus, 28 janvier 2022, consulté le 29.01.22, lien

[11] US Department of Treasury, « Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange », 8 novembre 2021, consulté le 20.01.22lien

pour utiliser un outil numérique comme arme de déstabilisation est de revenir au rôle principal du cyberespace : le partage d'informations. Quoi de mieux que des informations compromettantes sur une entreprise, un individu ou une institution, exposées au grand jour, et en libre accès ? En juin 2013, Edward Snowden, un ancien consultant de la NSA, dévoile, documents à l'appui, la façon dont la NSA a capté des métadonnées d'appels téléphoniques aux États-Unis, afin de collecter des informations. De la même manière, le site WikiLeaks publie des documents classifiés obtenus *via* des sources anonymes : les Guantanamo Files en 2008, des rapports militaires sur la guerre en Irak et en Afghanistan en 2010, rapports confidentiels de la NSA sur l'écoute téléphonique de trois anciens présidents français en 2016, etc.

Les moyens pour obtenir des données restent cependant encore nombreux : intelligence artificielle, OSINT et veille, etc.

3. Les impacts

Les moyens pour atteindre son adversaire se sont multipliés de manière exponentielle, et tous les acteurs (une simple PME comme une grande entreprise privée, ou un gouvernement) doivent réévaluer le niveau de risques que présente le développement du secteur numérique. Le risque d'attaque est beaucoup plus élevé et beaucoup moins prévisible. Leur variété augmente la difficulté des acteurs à les anticiper et à les contrer. Le cyberespace devient ainsi un champ de bataille, et les outils numériques les armes pour combattre : on peut parler de cyberguerre. Jean-Louis Gergorin[12] la caractérise comme une guerre qui « inclut les actions ou les préparatifs de cybersabotage, et la guerre numérique de l'information [et donc] les actions malveillantes destinées à menacer de paralyser ou de saboter effectivement les systèmes d'information civils et militaires ou les points névralgiques d'un État, comme ses infrastructures énergétiques ou de transport, en rendant inopérants ses liaisons et ses réseaux informatiques ; et, d'autre part, la manipulation des réseaux sociaux ou d'autres vecteurs numériques. (...) ».

Cela bouleverse totalement la manière dont on cherche à déstabiliser d'autres acteurs : le virus Stuxnet, développé dès 2007 par les États-Unis avec Israël, a ciblé le programme nucléaire iranien, et plus particulièrement la centrale de Natanz (site d'enrichissement d'uranium) et ses centrifugeuses. Le virus informatique a permis la destruction de plusieurs centaines de centrifugeuses[13]. L'attaque aurait permis de retarder le programme nucléaire

[12] Jean-Louis Gergorin, « Cyberespace: nouveaux défis, nouveaux risques », *Vie-publique.fr*, 13 novembre 2019, consulté le 24.01.22, lien
[13] M. Jean-Marie Bockel, « La cybersécurité : un enjeu mondial, une priorité nationale », *Rapport d'information du Sénat*, 18 juillet 2012, consulté le 02.02.22, lien

militaire de l'Iran de six mois à deux ans.[14] Selon un article de l'OBS, « les responsables du programme ont présenté dans la *situation room* des débris d'une de ces centrifugeuses : *"La preuve du pouvoir potentiel d'une cyberarme"* »[15]. Les cyberattaques n'ont pas seulement un impact dans le monde numérique, mais ont aussi des conséquences dans le monde réel, qui peuvent durer sur un plus ou moins long terme.

Enfin, de cette nouvelle façon de s'affronter découle une augmentation du marché des attaques numériques : une économie souterraine se développe en parallèle de l'économie légale, dans les couches plus profondes du cyberespace (*darkweb*, *deepweb*). Cela concerne des commandes d'attaques, mais aussi la revente illégale des données piratées.

On observe une transformation du cyberespace comme zone d'échange et de connectivité à une zone de conflits, d'attaques et de renversement de la souveraineté. Cela pose la question de la responsabilité pénale, et de l'encadrement juridique du numérique et du monde cyber.

Frontières numériques et souveraineté : comment la législation autour du cyberespace participe à son instrumentalisation

1. Quel cadre juridique et quelle protection pour le cyberespace en France ?

Le 3.3.3.1. de l'article 65 de la Loi n°2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019-2025 et portant diverses dispositions intéressant la Défense indique que « le développement du cyberespace à l'échelle planétaire, la rapidité d'accroissement de la dépendance au numérique de nos moyens militaires ainsi que l'extension des risques d'attaque sur nos systèmes électroniques, nécessitent le développement de capacités de cyberdéfense dans toutes leurs dimensions. Transverse aux fonctions stratégiques qu'elle soutient, la cyberdéfense porte en son sein un enjeu de souveraineté nationale »[16]. On peut donc voir que depuis quelques années, la cybersécurité est devenue l'un des enjeux stratégiques prioritaires de l'Union Européenne et de la France, notamment avec l'augmentation massive d'actes criminels dans le cyberespace.

[14] *Ibid*.
[15] Martin Untersinger, « Stuxnet : comment les Etats-Unis et Israël ont piraté le nucléaire iranien », *https://www.nouvelobs.com/rue89/*, 17 novembre 2016, consulté le 02.02.22, lien
[16] Loi n°2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025, consulté le 02.02.22, lien

Avec l'aide des agences nationales de cybersécurité, les autorités européennes ont préparé le *Cybersecurity Act*, qui pose un cadre législatif de cybersécurité pour l'espace européen. Les dispositions présentes au sein du règlement ont donc dû être transposées dans la loi nationale. Il est entré en vigueur le 27 juin 2019. Divisé en deux parties, le *Cybersecurity Act* officialise dans un premier temps le rôle de la *European Union Agency for Cybersecurity* (ENISA) comme institution officielle de l'UE pour la cybersécurité. La seconde moitié introduit un cadre européen de certification de cybersécurité pour « harmoniser à l'échelle européenne les méthodes d'évaluation et les différents niveaux d'assurance de la certification »[17]. Ces certifications sont reconnues dans toute l'UE. L'organisation de la cyberdéfense française s'est également structurée autour de la création de l'ANSSI en 2009 ainsi que du Commandement de la Cyberdéfense (COMCYBER) en 2017, qui est la force de cyberdéfense de l'armée française. En parallèle, la loi de programmation militaire (LPM) 2019-2025 prévoit un budget de 1.6 milliard d'euros pour la cyberdéfense[18]. Identifier les menaces afin de mieux pouvoir les contrer permet au modèle français de cyberdéfense d'être consolidé[19]. Pour la France, il ne peut y avoir de souveraineté numérique sans capacité d'autonomie numérique.

2. Un accord multilatéral manquant pour réellement réguler le cyberespace et la cybercriminalité ?

À l'heure actuelle, aucun accord multilatéral n'a encore été trouvé afin de pouvoir structurer et établir des normes communes et contraignantes pour les différents acteurs du cyberespace. Ce dernier n'est cependant pas dépourvu de règles juridiques. Le groupe d'experts gouvernementaux des Nations Unies (GGE) a publié différents rapports, qui ont permis d'indiquer que le droit international, et notamment la Charte des Nations-Unies, est applicable au cyberespace. En 2015, le groupe a développé un cadre normatif contenant des normes de comportement responsable, qui indiquent ce que les États devraient et ne devraient pas faire dans le cyberespace. Le 12 mars 2021, via la résolution 73/27, les États membres des Nations Unies ont adopté le rapport final de de l'*Open-ended working group* (OEWG), un groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications. Ce dernier réaffirme l'application des règles et normes évoquées précédemment, et souligne l'importance des États de faire preuve de transparence sur leur organisation en cybersécurité.

[17] ANSSI, Informations sur le Cybersecurity Act, consulté le 02.02.22, lien
[18] Les Echos, « Cyberdéfense : l'armée française étoffe ses troupes de cybercombattants », *Les Echos*, 9 septembre 2021, consulté le 02.02.22, lien
[19] *Revue stratégique de cyberdéfense*, 12 février 2018, p.48, consulté le 02.02.22, lien

Les désaccords restent cependant nombreux et la création d'un traité international sur le sujet reste incertaine, preuve d'un multilatéralisme défaillant sur le sujet. La question de la cybercriminalité est pourtant centrale dans l'ère numérique, et il est important de trouver des accords internationaux qui pourront davantage réguler le cyberespace.

Il est cependant possible de se demander si cela aurait une réelle utilité, puisqu'il est souvent difficile d'identifier ses attaquants et que les traités n'empêcheraient probablement pas les acteurs qui souhaitent s'affronter sur le cyberespace de le faire.

3. Quelles solutions pour protéger la souveraineté des acteurs ?

La protection de la souveraineté numérique des acteurs implique plusieurs enjeux : il faut sensibiliser et éduquer les individus et les entreprises, c'est-à-dire rendre la culture du numérique accessible et former pour anticiper les menaces. Le MOOC[20] de l'ANSSI est un bon exemple d'introduction aux notions de bases de la cybersécurité, qui permet aux particuliers de mieux comprendre les enjeux liés au cyberespace.

La souveraineté numérique passe par une amélioration constante des différentes priorités en matière de cyberdéfense. Ainsi, les systèmes d'information de l'État doivent être sécurisés le plus possible, car ce sont ceux qui contiennent les données les plus sensibles et importantes pour la sécurité nationale. De la même manière, les opérateurs d'importance vitale (OIV), soit les entités qui proposent des services indispensables à la survie de la nation, sont des piliers pour l'État français et doivent se conformer à des exigences informatiques, et acquérir les ressources nécessaires pour ne pas avoir de failles pouvant être exploitées à des fins criminelles. De manière générale, les différents types d'attaques possibles sur le cyberespace sont dues à des méconnaissances sur le sujet, notamment dans le cas des attaques de type *phishing*, ou à des mesures de cybersécurité insuffisantes. L'application d'un ensemble de règles de base et de normes permet d'éviter une majorité des attaques, cependant le risque n'est non seulement jamais inexistant, mais surtout, est en constante évolution.

En général, les États accompagnent les victimes de cyberattaques afin de les rendre plus résilientes, que ce soit des entreprises ou des particuliers, en mettant des moyens et et des ressources à disposition afin de les accompagner et de les aider à mieux se défendre face à tous types d'attaquants.

[20] https://secnumacademie.gouv.fr/

Conclusion

L'instrumentalisation du cyberespace à travers l'utilisation d'outils numériques est inévitable. L'interconnectivité, les évolutions, et les améliorations constantes n'offrent que toujours plus de moyens de le détourner de son usage premier, avec des conséquences pouvant être extrêmement importantes. On ne peut en effet pas isoler les rivalités présentes sur le cyberespace des rivalités politiques, culturelles, idéologiques présentes dans notre monde. Dès lors, l'utilisation qui est faite du cyberespace pourrait être considérée comme une retranscription de valeurs et de modes de pensée variés, qui se heurtent et qui soulèvent des désagréments pouvant mener à des escalades, voire à des conflits, et en cela, le manque d'encadrement juridique international devient une porte ouverte pour de nombreux attaquants.

Selon l'ANSSI, le nombre de cyberattaques a été multiplié par quatre en 2020[21], l'accroissement de l'importance accordée au cyberespace, à ses risques et menaces et à la place de la cyberdéfense dans la structure de l'État français est donc symbolique d'un paradoxe : là où les progrès numériques et technologiques sont en constante évolution, les attaques le sont aussi. La numérisation progressive et continue de la société paraît donc inéluctable parce qu'indispensable. Le cyberespace va continuer à être utilisé à des fins personnelles, mais aussi à des fins hostiles, auquel cas il pourrait presque être considéré comme une zone de non-droit, qu'il paraît impossible de réguler. Il est donc important pour ses utilisateurs de prendre conscience des dangers qu'il peut représenter, et d'apprendre à s'en protéger au maximum ; et pour les acteurs engagés dans des affrontements de coopérer lorsque cela est possible, afin d'assurer leur sûreté.

[21] ANSSI, L'ANSSI et le BSI alertent sur le niveau de la menace cyber en France et en Allemagne dans le contexte de la crise sanitaire, consulté le 02.02.22, lien