UNIVERSITÉ DU QUÉBEC À MONTRÉAL

« DIGITALISATION » DES FORCES ARMÉES : ENJEUX DE SÉCURITÉ NATIONALE ET INTERNATIONALE LIÉS À L'UTILISATION DE MATÉRIEL INFORMATIQUE DANS LE CADRE D'OPÉRATIONS STRATÉGIQUES ET MILITAIRES

TRAVAIL DE RECHERCHE DIRIGÉ
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN SCIENCE POLITIQUE

PAR
AUDE ROMPRÉ

AVRIL 2022

REMERCIEMENTS

Je tiens tout d'abord à remercier mes parents et mes amis, qui ont tous eu, à leur manière, leur façon de m'encourager à poursuivre des études supérieures en contexte pandémique ainsi que pour tout le support moral offert tout au long de ma maîtrise et de la rédaction de ce travail dirigé. Je veux également et plus particulièrement remercier mon père, Guillaume Rompré, dont l'expertise en informatique et en cybersécurité m'ont permis de définir adéquatement certains concepts propres à ce domaine et à mieux choisir et analyser les cas de figures qui ont été étudiés dans le cadre de ce travail dirigé.

Ensuite, je tiens à remercier mon directeur de travail dirigé, monsieur Ting-Sheng Lin, pour sa patience, sa disponibilité et ses multiples conseils prodigués tout au long du processus de rédaction du présent travail dirigé, et ce, dès le moment où je suis entrée en contact avec lui pour lui proposer de diriger mon travail et lui parler du sujet que je voulais étudier. Je veux aussi remercier monsieur Éric Boulanger qui, de concert avec monsieur Lin, a sû me donner différents conseils et commentaires quant à l'orientation et à la formulation de ce travail.

RÉSUMÉ

Les différentes technologies ainsi que les différents outils informatiques développés au cours des dernières années ont évolué plus rapidement que leur cadre juridique - qui est maintenant anémique et inadéquat au contexte actuel - , si bien que leur utilisation pour mener des cyberattaques - que ce soit par des particuliers ou par des États - créent de plus en plus d'enjeux politico-juridiques de sécurité internationale, surtout lorsqu'ils sont mobilisés par des États pour mener des attaques contre d'autres États dans le cadre de conflits stratégiques et militaires plutôt que des armes traditionnelles pour des raisons stratégiques, économiques et politiques, comme dans les cas classiques de la Russie contre l'Estonie en 2007 et de l'Opération Olympic Games en 2011. Il y sera donc questions des motifs expliquant pourquoi de plus en plus d'États ont recours aux cyberarmes et aux cyber unités de combat pour mener des opérations stratégiques et militaires, de leurs effets sur la scène internationale ainsi que des conséquences d'un manque d'encadrement juridique adéquat en droit international en la matière, du recours aux cyberarmes et du manque d'initiatives pour traiter de ces enjeux politico-juridiques de sécurité internationale tant pour les États que pour la population civile.

Mots-clés: cyberarmes, cyberattaque, cyberguerre, StuxNet, sécurité internationale, droit international, relations internationales

TABLE DES MATIÈRES

Introduction 4

Chapitre 1 : Nouvelles technologies, nouveaux enjeux 8

1.1. Définitions politico-juridique liées au cyberespace 8

1.2. Le choix de digitaliser les corps militaires 13

1.3. Portrait global des principaux enjeux de sécurité nationale et internationale liés au cyberespace et à l'utilisation de nouvelles technologies 16

Chapitre 2 : Dimension politique des enjeux autour de l'utilisation de matériel technologique à des fins stratégiques et militaires 20

2.1. Principaux corps militaires digitalisés : fonctions, budget, implications 20

2.2. Conséquences réelles et potentielles du recours aux cyberarmes : rapports de force, dommages collatéraux et dommages intentionnels 24

2.3. Cyberattaques étatiques importantes 29

2.4. Recommandations politiques d'améliorations en matière de traitement d'enjeux de cybersécurité 32

Chapitre 3 : Dimension juridique des enjeux autour de l'utilisation de matériel technologique à des fins stratégiques et militaires 36

3.1. Cadre juridique actuel 36

3.2. Enjeux principaux liés au cadre juridique actuel. 40

3.3. Cyber espionnage : stratégies et limites. 43

3.4. Recommandations juridiques d'améliorations en matière de traitement d'enjeux de cybersécurité. 46

Conclusion 49

Bibliographie 53

Introduction

Le recours aux technologies de pointe dans le cadre d'opérations stratégiques et militaires a toujours été au cœur des préoccupations des plus grands stratèges de l'Histoire, leur permettant de conquérir davantage d'espaces, de dominer des civilisations entières et de protéger leurs acquis le plus efficacement possible. Au cours du vingtième siècle, cette course aux armements et au développement de nouvelles technologies s'est intensifiée, nous donnant les premiers prototypes d'armes nucléaires et d'appareils dont on sous-estimait, à l'époque, les capacités destructrices que le cerveau humain sera capable de lui conférer. Tel fut le cas de ce qu'on appellerait aujourd'hui l'ordinateur.

Les premiers cas documentés de recours aux ordinateurs dans le cadre d'opérations stratégiques et militaires datent de la Seconde Guerre mondiale, notamment avec Enigma. Enigma était une machine développée par l'armée allemande s'apparentant à un ordinateur pouvant encrypter des messages contenant des informations sensibles, comme la date et le lieu de leurs prochaines frappes. Le but d'Enigma était de pouvoir envoyer discrètement ces messages aux autres services de renseignements allemands sans que ces messages puissent être interceptés par des services de renseignements ennemis[1]. Les services secrets britanniques ont d'ailleurs passé le gros de la Seconde Guerre mondiale, avec l'aide du célèbre Alan Turing et de son équipe, à développer Bombe, une machine pouvant décrypter les messages envoyés par Enigma via un algorithme, semblable à sa contrepartie polonaise éponyme. Après Bombe et Enigma, il y a également eu Delilah, une machine développée par Alan Turing également en partenariat avec l'armée américaine vers 1943 pour encrypter des messages vocaux[2].

Depuis, ayant compris la grande portée que de tels atouts technologiques peut avoir pour un État dans l'inventaire de ses forces armées et de ses services secrets, de plus en plus de gouvernements à travers le monde ont décidé de doter leurs corps armés et leurs services de renseignements d'outils informatiques à la fine pointe de la technologie. Ils ont aussi décidé de faire des investissements massifs à dans la recherche et le développement de nouveaux types d'outils à utiliser pour garder leur place dans les rivalités des relations internationales et pour en convoiter une meilleure. Parmi ces champs de recherche et de

[1]Imperial War Museum. (2021) [s.d.] *How Alan Turing Cracked the Enigma Code?* Récupéré de : https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

[2]Britannica, T. Editors of Encyclopaedia (2021, 2 août). Enigma. In *Encyclopedia Britannica*. Récupéré de : https://www.britannica.com/topic/Enigma-German-code-device

développement susmentionnés, on y retrouve, par exemple, l'étude poussée du plein potentiel technologique d'infrastructures, de logiciels, de langages et d'appareils informatiques couramment utilisés dans la vie de tous les jours tant par les citoyens lambdas que par les membres des institutions gouvernementales d'États en particulier, et plus encore. Des experts politiques en matière de cybersécurité écrivent:

> In the future, wars will not just be fought by soldiers with guns or with planes that drop bombs. They will also be fought with the clock of a mouse half a world away that unleashes carefully weaponized computer programs that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships[3].

C'est ainsi qu'au cours des vingt dernières années - et plus particulièrement les 10 dernières - les cyber unités de combat, les cyber espions et les cyberarmes ont rapidement gagné en popularité auprès d'États comme les États-Unis, la Russie, la Chine, la France, l'Australie, le Canada, le Pakistan, l'Inde et la Corée du Nord, pour n'en nommer que quelques-uns.

Bien que les chefs d'État commencent de plus en plus à apprivoiser les cyberarmes, leur trouvant des vertus intéressantes et importantes, il reste qu'une tendance inquiétante existe toujours, soit celle de l'incompréhension du sujet par les dirigeants politiques, qui sont souvent des personnes n'étant pas très familières avec les différents types de technologies ni avec les différents enjeux de sécurité que ces technologies peuvent poser. Singer et Friedman rapportent les propos d'un ancien directeur de la CIA quant au résultat d'une telle ignorance en la matière et d'un refus de s'informer sur le sujet :

> Rarely has something been so important and so talked about with less and less clarity and less apparent understanding...I have sat in *very* small group meetings in Washington…. unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long term legal and policy implications of any decision we might make[4].

Même plus de 30 ans après qu'Internet ait été rendu complètement public et ait conquis notre quotidien, il reste que pour plusieurs personnes importantes qui ne sont pas issues de la communauté des technologies de l'information et des communications (TIC) - comme les dirigeants politiques, les chercheurs en sciences sociales, les juristes, etc. - , les questions

---

[3]Singer, P.W., et Friedman, A. (2014) *Cybersecurity and Cyberwar: What everyone needs to know*, New York, Oxford University Press, 2014. (p.4)

[4] Ibidem, p.4

technologiques restent ésotériques et floues ; ces personnes mentionnées ci-haut sont donc découragées de tenter de comprendre ces questions technologiques et d'en saisir l'importance sur l'évolution de la situation internationale politique, juridique, économique, militaire et sociale actuelle. Malgré ces craintes d'appréhender les questions technologiques dans une salle de réunion ou dans un laboratoire de recherche, depuis une quinzaine d'années - soit depuis une montée exponentielle du nombre de cyberattaques à travers le monde et du recours aux cyberarmes dans le cadre d'opérations stratégiques et militaires par de nombreux États - , il est possible d'observer une hausse marquée du nombre de recherches en sciences sociales et en sciences informatiques portant sur ce sujet d'actualité. On peut lire à ce propos que :

> [...] les cyberattaques et les cyberarmes sont tellement prisées par les États qu'elles seront éventuellement des incontournables pour éviter qu'un corps armé ne perde sa crédibilité, de sa pertinence et de sa puissance aux yeux de la communauté internationale. De plus, comme ces technologies se développent à une vitesse exponentielle beaucoup plus grande que le cadre juridique en matière de droit martial, de droit international humanitaire et de droit informatique, de nombreuses failles dans le cadre juridique actuel en matière d'encadrement de l'usage de cyberarmes se creusent et méritent d'être étudiées par les juristes de la communauté scientifique[5].

Considérant la situation actuelle ainsi que son évolution, à la lecture de la littérature existante, la question suivante mérite d'être explorée : comment, au cours des dernières décennies, la digitalisation des opérations stratégiques et militaires via l'utilisation de matériel informatique a-t-elle contribué à créer de nouveaux enjeux de sécurité nationale et internationale ? Il est possible de dire que des dizaines d'enjeux politiques et juridiques liés au recours à du matériel informatique et aux nouvelles technologies dans le cadre d'opérations stratégiques et militaires se sont créés au fil des ans - et que d'autres risquent d'apparaître également avec l'avènement d'autres technologies plus sophistiquées - et gagnent à ce que la communauté scientifique y porte une attention particulière. On peut penser entre autres à l'identification et le contrôle des cyberarmes, l'adoption d'une définition politique et juridique claire et reconnue par la communauté internationale d'une cyberattaque, d'une cyberarme et du cyber espionnage ainsi que les conséquences sociales, économiques, et politiques tant pour les États que pour la population civile de l'utilisation de cyberarmes.

---

[5] Rompré, A. (2021) *Digitalisation des forces armées: enjeux de sécurité nationale et internationale liés à l'utilisation de matériel informatique dans le cadre d'opérations stratégiques et militaires*. [Projet de travail dirigé, document non publié]. Université du Québec à Montréal.

Utilisant une approche s'inspirant du réalisme pour étudier les enjeux mentionnés ci-haut, la présente réflexion se déclinera en trois volets : d'abord, il sera question de la définition technique de cinq concepts-clés communs aux enjeux politico-juridiques qui seront étudiés plus tard, puis deux chapitres seront alloués respectivement aux principaux enjeux politiques et juridiques de cybersécurité internationale ayant rapport au recours aux cyberarmes. Cette réflexion se clôturera sur une ouverture vers une autre portant sur d'autres avenues à explorer dont il n'aura pas été question dans ce texte, étant donné les contraintes matérielles de ce dernier.

Chapitre 1 : Nouvelles technologies, nouveaux enjeux

1.1. Définitions politico-juridique liées au cyberespace

Afin de pouvoir bien saisir l'ampleur et la nature des enjeux politico-juridiques de sécurité internationale liés au recours des cyberarmes et de bien comprendre ce dont il sera question tout au long de cette réflexion, il est important de définir les concepts-clés liés aux thèmes qui y seront abordés, les nuances entre celles-ci et en quoi ils se distinguent les uns des autres. Bien qu'il faille s'attendre à certaines définitions directes et claires, il existe toutefois une sorte de zone grise autour d'autres définitions importantes. Pour le bien de cette recherche, et considérant les limites spatio-temporelles qui y sont allouées, cinq concepts-clés seront retenus et étudiés plus en profondeur ; il s'agit des concepts de cyberespace, de cybersécurité, de cyberattaque, de cybercriminalité et de cyberarmes.

La définition du cyberespace la plus inclusive, simple et directe est celle donnée par le ministère de la Défense français. Ils le décrivent comme suit :

> Le cyberespace est un domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunication, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs de services en ligne[6].

Le cyberespace serait donc cette espèce de grand environnement invisible dans lequel est catalogué tous nos renseignements personnels intangibles (dont les données des applications et des appareils technologiques que nous utilisons sur une base quotidienne), nos fichiers et nos publications numériques que nous téléversons dans le World Wide Web, le dark web, les différentes pages de réseaux sociaux, les nuages informatiques (*cloud*, *drive*) et les bases de données partagées et/ou publiques.

Chaque gouvernement a la possibilité de légiférer sur une partie du cyberespace, notamment en limitant l'accès à certains types de contenus à ses citoyens, mais la réalité est beaucoup plus complexe : en prohibant certains contenus, moteurs de recherche et/ou applications, ces gouvernements se font critiquer sur la place publique depuis une dizaine d'années par la population et par d'autres États parce que ce contrôle du cyberespace irait à l'encontre de la neutralité de celui-ci.

---

[6]Ministère des Armées. [s.d.] *La cyberdéfense*. Récupéré de : https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/mission

> Dans le virage qu'a constitué la conférence de l'UIT à Dubaï, l'excessive polarisation entre les partisans d'un internet « libre et ouvert » et les tenants d'une gouvernance fondée sur la souveraineté territoriale avait suscité un discours anxiogène autour d'une possible « guerre froide numérique » […]. Durement éprouvés, les mécanismes actuels de gouvernance pour conserver une légitimité sur le long terme, devront prendre en considération les revendications [d'acteurs émergents][7].

Étant donné la vastitude du cyberespace ainsi que la quasi-absence de régulations nationales et internationales le régulant, tel un *no man's land* virtuel, le cyberespace semble devenir un champ de bataille intéressant pour les États où presque tous les coups sont permis. Dans les faits, comme l'expliquent Signer et Friedman, la notion géopolitique de frontières existe également dans le cyberespace et est très mal comprise autant par les utilisateurs lambdas que par les hackers, les juristes et les décideurs politiques : en effet, bien que ces frontières ne sont évidemment pas physiques et tangibles, et que celles-ci sont en constante évolution, les mêmes frontières géopolitiques et géographiques existantes dans le monde réel existent également dans le cyberespace dans les mêmes conditions que dans le monde tangible pour pouvoir permettre aux États d'y exercer leurs droits et leurs devoirs, comme l'exercice de sa souveraineté, par exemple[8].

La définition large donnée par la communauté des TIC - technologies de l'information et des communications - de la cybersécurité est l'ensemble des pratiques et des outils mis à la disposition des utilisateurs de réseaux et de matériel informatiques ainsi que d'appareils intelligents en tout genre (ordinateurs, téléphones, tablettes, etc.) pour protéger leurs données et leurs fichiers contre toute potentielle menace à la sécurité de ces utilisateurs en question. Il peut s'agir, par exemple, de murs pare-feux (*firewall*), de logiciels anti-virus, de différents types de mots de passe uniques générés automatiquement aux utilisateurs à une fréquence précise, de protocoles de sécurité détaillés, d'encryption de fichiers, etc.

Toujours selon Singer et Friedman, il y aurait trois grands buts canoniques de la cybersécurité, ce qu'ils appellent en anglais «the CIA triad» : la confidentialité, l'intégrité et la disponibilité (availability) des systèmes d'exploitation tel que ce à quoi on s'attend de ceux-ci. (Signer et Friedman, p.35) À ce sujet, ils définissent la cybersécurité ainsi,

---

[7] Nocetti, J. (2014). Puissances émergentes et internet : vers une « troisième voie » ?. In *Politique étrangère*, numéro 4 , 43-55. DOI: https://doi.org/10.3917/pe.144.0043

[8] Singer, P.W., et Friedman, A. (2014) *Cybersecurity and Cyberwar: What everyone needs to know*, New York, Oxford University Press, 2014. (p.14)

démystifiant certaines idées préconçues que des personnes non-expertes en informatiques pourraient avoir:

> Security isn't just the notion of being free from danger, as it is commonly conceived, but it is associated with the presence of an adversary. In that way, [...] you need at least two sides to make it real. Things may break and mistakes may be made, but a cybersecurity issue if an adversary seeks to gain something from the activity, whether to obtain private information, undermine the system, or prevent its legitimate use[9].

Ces mesures sont mises en place surtout pour éviter les menaces extérieures à l'utilisateur, comme une tentative de piratage d'un système par un individus ou un groupe de hackers, mais aussi pour prévenir les menaces provenant de l'intérieur d'une organisation en particulier : en effet, la plupart des brèches de sécurité d'un système informatique sont causées par l'erreur humaine, que ce soit par des systèmes de sécurité obsolètes - c'est-à-dire dont les mises à jour n'ont pas été faites et/ou qui n'est pas adapté aux nouvelles potentielles menaces - , le fait d'avoir le même mot de passe pour tous les comptes (ex.: accès à une application ou à un logiciel qu'un individu posséderait, avoir un mot de passe facile à deviner (date de naissance, date d'anniversaire de mariage, nom du/une conjoint-e, nom des enfants, etc.), un mot de passe inscrit sur un bout de papier, et plus encore[10]. Ces types d'erreurs humaines susmentionnées coûtent chaque année des milliards de dollars tant au secteur privé qu'aux institutions gouvernementales d'à travers le monde, et ce, malgré les formations données régulièrement par les ressources humaines d'entreprises et d'agences gouvernementales en matière de cybersécurité et malgré le faible coût, à longs termes, d'une protection adéquate de son parc informatique.

Une cyberattaque est définie comme « l'ensemble coordonné d'actions malveillantes conduites par l'intermédiaire du cyberespace, qui visent à endommager, à forcer ou à détourner un réseau ou un système informatique afin de commettre un acte préjudiciable.[11]» Ces attaques virtuelles peuvent être conduites, par exemple, dans le but de voler des données confidentielles pour en tirer un certain profit ensuite (comme dans le cas de la cyberattaque

---

[9] Singer, P.W., et Friedman, A. (2014) *Cybersecurity and Cyberwar: What everyone needs to know*, New York, Oxford University Press, 2014. (p.34)

[10]Exportation et Développement Canada. (2018, 24 janvier) La gestion des cyber risques : un sujet incontournable en 2018. In *ExportActions*. Récupéré de : https://www.edc.ca/fr/article/2018-cyber-risk-management.html

[11]Office québécois de la langue française. [s.d.] *Cyberattaque*. Récupéré de : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8351162

contre le regroupement Desjardins il y a trois ans[12]), pour modifier ou endommager un système en place, pour épier des membres en particulier d'une entreprise ou d'une organisation quelconque via leur parc informatique et leurs appareils intelligents, etc. Il existe des dizaines de types de cyberattaques différentes en fonction des moyens et des techniques utilisés, du but ainsi que des cibles - organisations, personnes morales, personnes physiques, etc. - de ladite attaque.

Les techniques les six plus communes sont le phishing, soit l'hameçonnage d'une victime via un courriel qui pourrait sembler, à première vue, à un courriel légitime d'une organisation, d'une entreprise ou d'une personnes existante ; l'exploitation «zero day», qui porte son nom dû au fait que c'est le jour 0 de la mise à nue et de l'exploitation d'une vulnérabilité dans le système informatique d'une organisation X par l'attaquant ; les malwares, qui sont des logiciels, des applications, des codes, des fichiers et/ou d'autres éléments malveillants qui vont infecter les systèmes d'exploitation dans lesquels ils sont relâchés, installés et/ou sauvegardés ; les injections SQL (Structured Query Language; communément appelé aussi «sequel»), qui piège une victime en lui faisant exécuter la commande voulue par l'attaquant plutôt que celle voulue initialement par la victime pour envahir une base de données en voler son contenu[13]; les DdOS (distributed denial of service), qui ont pour but de neutraliser une cible en envoyant, depuis un grand nombre de sources différentes, une charge de travail trop lourde pour les capacités de celles-ci ; et, enfin, les MITM (man in the middle) - où une tierce partie intercepte discrètement les communications et les échanges entre deux autres parties sans qu'elles ne s'en rendent compte, qui arrive souvent entre autres lorsque ces parties utilisent des connexions non-sécurisées pour faire ces échanges et ces communications. Une cyberattaque peut combiner plus d'une technique, dépendamment des habiletés de l'attaquant, de ses cibles à atteindre et des dommages qu'il souhaite causer : par exemple, si un attaquant voulait obtenir toutes les données biométriques d'une population en particulier qui sont contenues dans une base de données gouvernementales pour pouvoir les revendre sur le darknet ou à d'autres agences de renseignements, cet attaquant pourrait combiner presque toutes les techniques susmentionnées

[12] Boily, D. (2021, 8 décembre) Vol massif de données : l'ex-employé aurait tout avoué à la direction de Desjardins. In *Radio-Canada Informations*. Récupéré de : https://ici.radio-canada.ca/nouvelle/1845776/vol-massif-donnees-ex-employe-confession-direction-desjardins

[13]Singer, P.W., et Friedman, A. (2014) *Cybersecurity and Cyberwar: What everyone needs to know*, New York, Oxford University Press, 2014. (p.42)

- à l'exception du DdOS - pour arriver à ses fins et endommager davantage l'infrastructure de la base de données qu'il vient de piller au passage.

À l'heure actuelle, la définition la plus communément utilisée pour décrire ce qu'est la cybercriminalité - qui est utilisée, entre autres, par la Gendarmerie royale du Canada - est l'ensemble des activités illégales perpétrées à travers l'utilisation de matériel informatique et technologique, comme Internet, les ordinateurs en tout genre, les téléphones intelligents, les tablettes, etc[14]. Cette définition, bien qu'elle soit plutôt vague, n'est toutefois pas la même partout, variant du code criminel d'un État à un autre (lorsque cet État reconnaît l'existence de la cybercriminalité) et d'une convention ou d'un traité à un autre: on peut citer, par exemple, la Convention de Budapest de 2001, qui est entrée en vigueur en 2004 et qui est le seul document juridique en droit international qui traite directement de la cybercriminalité. Les crimes sanctionnés par cette convention sont l'atteinte aux droits d'auteurs, la pédopornographie, la fraude informatique et le trafic ainsi que le vol de données stockées sur du matériel informatique à des fins illégales[15]. (Convention de Budapest, 2001) Cela signifie que certains actes criminels ne sont donc pas concernés par la définition susmentionnée, tels que la cybersurveillance, le cyberespionnage (sauf dans certains cas où celui-ci est fait dans le cadre de l'utilisation illégale des données susmentionnées, ce qui est également flou juridique à part entière), le cyberterrorisme et d'autres types de cyberattaques.

Si on se fie à la définition-même de la cybercriminalité qui a été étudiée au paragraphe précédent, il irait de soit de croire que les cyberarmes sont, grosso modo, n'importe quel outil technologique utilisé dans le cadre d'une cyberattaque. Toutefois, ce n'est tout le cas à fait le cas: en théorie, selon le *Talinn Manual on International Law Applicable to Cyber Warfare*, une cyberarme est un moyen technologique utilisé dans le cadre d'un conflit choisi pour sa capacité, que ce soit dans l'intention d'utilisation et/ou dans son design, de causer des dommages (blessures, destruction, gel, etc.) à des personnes et/ou à des infrastructures semblables à ceux causés par des armes conventionnelles inscrits dans la Convention de Genève de 1949 et dans la Convention de La Haye de 1954. Dans un article paru en 2015, Clay Wilson, expert en cybersécurité, nomme quatre caractéristiques communes pouvant

[14]Gendarmerie royale du Canada. (2014) *Cybercriminalité : survol des incidents et des enjeux au Canada*. [Rapport] https://www.rcmp-grc.gc.ca/fr/cybercriminalite-survol-des-incidents-et-des-enjeux-au-canada >
[15]*Convention sur la cybercriminalité*, 2001, STE 185 –23.XI.2001 (entrée en vigueur le 1er juillet 2004) [Conseil de l'Europe]

aider la communauté à identifier adéquatement une potentielle cyber arme[16]: une campagne combinant plusieurs logiciels d'espionnage, de vol de données ou de sabotage ; un type de code informatique spécial capable d'outre-passer les protocoles de cybersécurité en place ; une capacité furtive de l'opération à compromettre un système ciblé tout en restant sous le radar des mécanismes de sécurité ; et, enfin, un attaquant ayant une connaissance intime apparente des détails du fonctionnement du système ciblé[17]. En pratique, malgré ces définitions et ces critères, la plupart des États de la communauté internationale ne vont reconnaître que les logiciels malveillants (malware) et les codes utilisés dans le cadre d'une cyberattaque comme une cyber arme et non l'ensemble des infrastructures informatiques et des appareils ayant contribué à réaliser ladite cyberattaque. C'est ainsi que, par exemple, dans le cas de la série de cyberattaques menées par les États-Unis à l'égard de l'Iran et de ses centrales nucléaires - dont il sera question plus en profondeur plus tard au cours de cette réflexion - seul Stuxnet (le code malveillant utilisé pour infecter le réseau de centrales nucléaires en question) est considéré comme une cyberarme, excluant, par exemple, l'ordinateur qui a servi à le coder et le matériel qui a servi à infecter les infrastructures informatiques iraniennes.

1.2. Le choix de digitaliser les corps militaires

Les motivations d'un acteur de digitaliser ses corps militaires et d'avoir recours aux cyberarmes sont très personnelles et varient d'un acteur à l'autre. Toutefois, il existe des raisons communes qui motivent les États à vouloir mettre sur pied des cyber unités de combat et à vouloir investir dans des cyberarmes. Découlant d'un judicieux calcul coût-bénéfices, voici les deux principales motivations de ces États pour entreprendre ce virage technologique.

En premier lieu, il est possible de dire que les États sont de plus en plus intéressés à investir dans les cyberarmes parce qu'il s'agit d'une solution qui est, certes, en vogue et en symbiose avec les multiples technologies disponibles sur le marché, mais surtout, car il s'agit d'une solution peu coûteuse, permettant de réduire les dépenses d'un État en matière de défense. D'abord, comme ces opérations digitalisées peuvent se faire à distance, les États n'ont pas besoin de payer des frais de transport pour déplacer des troupes ni de matériel tactique (incluant des véhicules, des armes et des munitions) sur un champ de bataille pour

[16]Wilson, C. (2015, 4 juin) Cyber Weapons : 4 defining characteristics. GCN. https://gcn.com/articles/2015/06/04/cyber-weapon.aspx
[17] Ibidem.

aller se battre contre un ennemi potentiel et aux côtés de leurs alliés. Tout peut se faire en quelques clics dans un bureau à même leur propre sol national.

Ensuite, les cyberarmes sont renouvelables (contrairement aux munitions traditionnelles) et ne requièrent pas un entretien aussi poussé que les armes traditionnelles: comme il s'agit généralement de logiciels ou de lignes de codes sur des ordinateurs ou sur d'autres appareils intelligents, il ne suffit que d'avoir quelques personnes formées en matière d'informatique et de cybersécurité qui s'assurent régulièrement que les mises à jour sur les appareils[18] soient faites et que les appareils soient en bon état pour pouvoir mener des opérations dans le cyberespace[19]. Il n'y a pas besoin, par exemple, d'une équipe de mécaniciens qui doivent régulièrement changer l'huile et les différentes pièces d'une flotte de véhicules, d'acheter régulièrement différents types de munitions (par milliers) et d'en faire l'inventaire, d'avoir une équipe de personnes qui s'assurent de l'entretien des différents fusils et du roulement de l'inventaire de l'artillerie, et plus encore.

D'ailleurs, lorsque nous analysons les dépenses budgétaires de différents ministères de la Défense à travers le monde en matière de cyber unités de combats et que nous comparons ces dépenses à celles pour d'autres corps armés du même État, les chiffres parlent d'eux-mêmes: par exemple, si nous analysons le budget du département de la Défense des États-Unis pour l'année 2021, il est prévu que pour l'ensemble des opérations de cyberdéfense et de cybersécurité, 9,8 milliards de dollars américains seront dépensés, contre 41,6 milliards de dollars seulement en munitions et en missiles pour les unités de combats de l'armée de terre, de l'armée de l'air et pour la marine américaine[20]. Il s'agit donc d'un bénéfice budgétaire et stratégique non négligeable pour les États que d'investir dans les cyberarmes et de digitaliser leurs corps armés.

En second lieu, dans un ordre d'idées similaires, il est possible de dire que certains États ont beaucoup à gagner en investissant dans la digitalisation de leurs corps armés. En effet, en raison du coût bas de ce type d'armements, des puissances émergentes, comme la Chine, et des acteurs qui sont considérés comme «plus petits» ou «moins imposants» par la

[18] Gouvernement du Canada. [s.d.] *Cyber Operator*. Récupéré de : https://forces.ca/en/career/cyber-operator/
[19] Coustillière, A. (2016). Le combat numérique au cœur des opérations : quels enjeux pour le monde maritime ? *Revue Défense Nationale*, 789, 44-48. https://doi.org/10.3917/rdna.789.0044
[20] United States' Department of Defense. [s.d.] *DOD Releases Fiscal Year 2021 Budget Proposal*. Récupéré de : https://www.defense.gov/News/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/

communauté internationale en matière d'affaires militaires peuvent se démarquer plus facilement au sein du système international beaucoup plus rapidement qu'auparavant, ayant maintenant accès à un armement puissant et peu coûteux, leur donnant l'opportunité sur le long terme de modifier les rapports de force asymétriques avec leurs rivaux, allant même jusqu'à leur donner l'avantage dans un lutte asymétrique de pouvoir. Traditionnellement, la course aux armements est une affaire d'États riches et puissants, capables d'asseoir leur domination sur le monde entier en assiégeant, en annexant et/ou en conquérant d'autres États, et en dissuadant les autres de les attaquer en démontrant les dommages physiques - comme le bombardement d'institutions importantes - et collatéraux - tuant au passage des civils - que peuvent causer leur artillerie et leurs flottes de véhicules de combat.

Avec les cyberarmes, des États comme l'Iran, le Pakistan et l'Inde, qui n'ont pas nécessairement les moyens de se payer une artillerie lourde ni une flotte de véhicules tactiques suffisamment puissantes pour dissuader des États perçus comme de « grandes puissances » au sein du système international - comme les États-Unis, la Russie et la Chine – d'entrer potentiellement en conflit avec eux peuvent enfin avoir le dessus sur ces grandes puissances. En effet, ceux-ci ont souvent l'expertise informatique et stratégique pour pouvoir mener à termes des cyberattaques complexes en exploitant les faiblesses et les failles technologiques de ces grandes puissances, dont leur manque de connaissance des enjeux de cybersécurité nécessaires à la protection adéquate de leurs secrets d'État ainsi que des données financières et biométriques de leurs contribuables. Ces puissances émergentes peuvent donc, par exemple, prendre en otage des institutions gouvernementales tout en volant les données et les renseignements sensibles dont ils ont besoin pour avoir l'avantage sur eux lors de négociations futures, sachant que leurs attaques coûteront des sommes faramineuses en reconstruction d'infrastructures pour leurs victimes : « Le coût de la cybercriminalité au Canada équivaut à 0,17% de son produit intérieur brut (PIB), ce qui représente des pertes annuelles de 3,2 milliards de dollars canadiens par année.» (CRPC, 2019) La collecte de renseignements sensibles via des cyberattaques donne donc le pouvoir aux plus petits acteurs étatiques pour notamment (re)négocier de nouvelles ententes sur divers enjeux et partenariats, pour leur faire du chantage et/ou les extorquer en cas de refus de coopération, pour connaître les stratégies et les plans d'actions d'une potentielle attaque physique avant qu'elle ne se produise, pour occuper un territoire en vue d'un futur conflit armé, et plus encore. Ces « petits acteurs » obtiennent ainsi souvent des résultats plus rapidement et plus satisfaisants qu'auparavant.

1.3. Portrait global des principaux enjeux de sécurité nationale et internationale liés au cyberespace et à l'utilisation de nouvelles technologies

Malgré les nombreux avantages que peuvent tirer les États d'une digitalisation de leurs corps armés ainsi que du recours au cyberarmes dans le cadre de leurs opérations stratégiques et militaires comme il en a été discuté dans la section précédente, il reste que les enjeux de cybersécurité internationale liés au recours aux cyberarmes se multiplient à la même vitesse exponentielle que le développement des technologies et leur disponibilité sur le marché international. Cette section de ce chapitre brossera un portrait global des principaux enjeux de sécurité nationale et internationale liés au cyberespace et à l'utilisation de nouvelles technologies, notamment ceux en lien avec l'applicabilité du droit international humanitaire (DIH) dans le cas de cyber opérations et du recours aux cyberarmes.

Tout d'abord, l'un des enjeux les plus importants tant sur les plans politique que juridique est le fait que certains États ne reconnaissent pas certains types de cybercrimes comme un crime au sein de leur droit national ni se sont dotés de moyens concrets et efficaces pour légiférer sur cette question, causant ainsi une absence de consensus sur une définition universelle et reconnue de la communauté internationale de ce que sont la cybercriminalité, la cybersécurité, les cyber opérations, les cyberarmes, et tous les concepts dont il a été question dans la toute première portion de ce chapitre. Tel que mentionné plus haut, depuis le début des années 2000, le seul texte de droit international en vigueur qui traite de la question de la cybersécurité et des cyberattaques est la Convention de Budapest, adoptée en 2001 et entrée en vigueur en 2004, qui sanctionne l'atteinte aux droits d'auteurs, la pédopornographie, la fraude informatique et le trafic ainsi que le vol de données stockées sur du matériel informatique à des fins illégales[21]. En date du 1er août 2021, seuls 66 États sur les 193 États-membres de l'Organisation des Nations unies[22] ont signé cette convention et intégré à leur droit interne une loi et/ou des règlements sur la cybercriminalité, et certains d'entre eux ne l'ont fait qu'assez récemment : c'est notamment le cas du Canada, qui a ratifié la Convention de Budapest en 2014 et qui a intégré des principes de cybercriminalité à son droit criminel que la même année. Le Pakistan, n'a fait de même qu'en 2016. Dans le cas des 66 États susmentionnés, il n'y a également pas vraiment de législation et de politiques nationales – ni d'initiatives internationales par le fait même - mises en place pour encadrer le recours aux

[21] *Convention sur la cybercriminalité*, 2001, STE 185 –23.XI.2001 (entrée en vigueur le 1er juillet 2004) [Conseil de l'Europe]

[22] Council of Europe. [s.d.] *Chart of signatures and ratifications of Treaty 185*. Récupéré de : https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

cyber armes dans le cadre de conflits armés ni d'opérations stratégiques et militaires, ce qui pourrait éventuellement faire des 130 États une cible particulière de cyberattaques étatiques. Cela signifierait également qu'en cas de cyberattaque interétatique, la Convention de Budapest ne s'appliquerait pas à certaines cibles particulières, puisque les principes fondamentaux de la Convention de Budapest ne pourront s'appliquer sur ces territoires non-signataires. Ces États ne peuvent donc pas traduire en justice les auteurs de cybercrimes et de cyberattaques à leur endroit, ce qui est une faille juridique et politique importante que beaucoup exploitent déjà en ce sens.

Toujours en lien avec le flou juridique dont il a été question dans le paragraphe précédent, un autre enjeu important à prendre en considération dans l'étude politico-juridique des cyberarmes dans le cadre d'opérations stratégiques et militaires est le principe de légitime défense et de riposte équivalente à une attaque selon le droit international humanitaire. Depuis la fin de la Seconde Guerre mondiale, le droit international humanitaire proscrit le recours à la force armée sauf dans quelques cas précis de dernier recours lorsque tous les autres moyens de règlement des différends ont échoué[23], comme en cas de légitime défense par exemple. Dans ce cas particulier, le jus ad bellum prévoit qu'un État victime d'une agression armée peut riposter à son attaquant avec une frappe d'une force proportionnelle à celle qu'il a reçue, c'est-à-dire que, par exemple, un État A qui se serait fait bombarder un petit village côtier par un État B ne pourrait répondre par une frappe tellement puissante qu'elle détruirait l'ensemble de la capitale de l'État B.

Selon le comité international de la Croix-Rouge (CICR), il ne fait nul doute que le droit international humanitaire reconnaisse les cyberattaques dans le cadre d'opérations stratégiques et militaires comme une infraction au droit international, comme tous les recours à la force armée entre deux États sans que ceux-ci n'aient épuisé tous les modes pacifiques de règlement des différends. Cependant, comme il n'est nullement question de façon directe dans le droit international de l'encadrement du recours aux cyber armes ni de la façon dont une cyberattaque étatique peut ou ne peut pas être conduite, il est longuement (et toujours) débattu par des juristes de l'applicabilité et de l'intervention du droit international humanitaire dans le cas d'un conflit strictement virtuel. Par exemple, si un État A lance une cyberattaque contre

[23]Comité international de la Croix-Rouge. [s.d.] *Traités, États parties et Commentaires - Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), 8 juin 1977.* Récupéré de : https://ihl-databases.icrc.org/dih-traites/COM/470-750056?OpenDocument

les infrastructures informatiques gérant les centrales nucléaires d'un État B, quels sont les recours de ce dernier en la matière ? Comment se mesure et se transpose la proportionnalité de la force d'une cyberattaque au monde physique ? Est-ce que l'État B pourrait clamer la légitime défense et exercer une frappe physique contre l'État A pour détruire ses centrales électriques ? Doit-il se contenter d'une cyberattaque aux effets similaires ? Après avoir observé de nombreuses cyberattaques d'États à États, le CICR rappelle l'importance du respect du droit international humanitaire pour prévenir et limiter les effets de cyberopérations militaires tant sur la population civile que sur les institutions étatiques[24]. Selon eux, il est également dans l'intérêt de tous les États de réglementer les cyber opérations menées durant un conflit armé, quel que soit leur degré d'avancement technologique, leurs cyber capacités militaires et leur participation à des conflits armés[25]. En réalité, comme il n'existe aucune jurisprudence en la matière et puisqu'aucun texte juridique comme tel ne fait état de la proportionnalité de la force des cyberattaques - ainsi qu'en l'absence en droit international de textes juridiques établissant clairement les sanctions en cas de violation de celui-ci - , il est difficile de trancher sur ce qui peut constituer de la légitime défense et ce qui constitue en soi une riposte proportionnelle en cas de recours aux cyberarmes dans le cadre d'opérations stratégiques et militaires. Tel que mentionné par le CICR, il est du devoir des États de créer un cadre juridique sur la question pour pouvoir mieux renforcer le droit international humanitaire en la matière.

Enfin, un dernier enjeu politico-juridique important à considérer dans l'étude du recours aux cyberarmes dans le cadre d'opérations stratégiques et militaires en lien avec les enjeux mentionnés plus tôt est le fait que les principales victimes des cyberarmes ne sont pas des membres de corps militaires, comme dans un combat traditionnel sur un champ de bataille, mais bien des membres de la société civile. En effet, chaque fois qu'une frappe avec des cyberarmes est menée, par exemple, à l'instar d'agences gouvernementales dans le but non seulement de les fragiliser et de les immobiliser, mais dans le but également d'en voler des secrets d'États et des données en tout genre, cette cyberattaque fait directement pour victimes (dans la très grande majorité des cas) des civils qui viennent de se faire voler leurs données sensibles aux dépens d'un conflit interétatique. Présentement, toujours selon le comité international de la Croix-Rouge, le droit international humanitaire prévoit que les actes

[24] Comité international de la Croix-Rouge. (2021, 25 février) *Le droit international humanitaire peut-il limiter la cyberguerre?* Récupéré de : https://www.icrc.org/fr/document/Le-droit-international-humanitaire-peut-il%20limiter-la-cyberguerre%3F
[25] Ibidem.

de guerre ne peuvent toucher des civils, directement ou indirectement, mais il n'est pas ou très peu renforcé en matière de cyberattaques étatiques en raison, comme dans le paragraphe précédent, d'un débat sur la personnalité juridique attribuées aux données des membres de la société civile. Le CICR rappelle aussi aux membres de la communauté internationale que le droit international humanitaire actuel prévoit déjà que celui-ci englobe tous les types de conflits armés et d'armements, même ceux qui n'existaient pas au moment de la mise en place des règles du droit international humanitaire[26]. Cela signifierait que de facto, les cyber armes, les cyberopérations et les cyberattaques sont encadrées par le droit international humanitaire[27]. Il est donc évident que malgré tous les avantages que représentent le recours aux cyberarmes pour les États dans le cadre de leurs opérations stratégiques et militaires, de nombreux enjeux importants touchant plus particulièrement la sécurité de leur société civile et l'applicabilité du droit international humanitaire sont également à prendre en compte pour éviter de compromettre la sécurité de l'ensemble du système international aux dépens de potentiels gains personnels rapides et faciles à obtenir.

[26] Durham, H. (2020, 26 mars) Les cyberopérations en période de conflit armé : 7 questions juridiques et politiques essentielles. In *CICR*. Récupéré de : https://blogs.icrc.org/law-and-policy/fr/2020/03/26/cyber-armed-conflict-7-law-policy-questions/

[27] Ibidem

Chapitre 2 : Dimension politique des enjeux autour de l'utilisation de matériel technologique à des fins stratégiques et militaires

2.1. Principaux corps militaires digitalisés : fonctions, budget, implications

Afin d'étudier adéquatement les enjeux politiques entourant le choix des États de se doter d'une cyber unité de combat et/ou d'une unité spécialisée en cybersécurité, il est important d'identifier qui sont les principaux corps militaires digitalisés ainsi que trois aspects sur lesquels notre étude portera pour démontrer en quoi ces corps militaires cybernétiques méritent une attention particulière. Cette réflexion se concentrera sur les cas de la Russie, de la Chine, des États-Unis et du Canada et analysera leur budget, les fonctions principales de leurs cyber unités (recherche, développement, surveillance, défense, etc.) et dans quels types de cyber opérations ces unités récemment été impliquées.

Les États-Unis sont actuellement considérés comme la plus grande puissance cybernétique du système international. Créé en mai 2010, le US Cyber Command est « responsable de la planification, de la coordination, de l'intégration, de la synchronisation et de la direction des activités d'exploitation et de défense des réseaux d'information du ministère de la Défense et, lorsqu'il y a lieu, de mener des opérations militaires complètes dans le cyberespace. » (CCDCOE, 2013) Tel que mentionné plus tôt au cours de cette réflexion, le ministère de la Défense a prévu un budget de 9,8 milliards de dollars américains pour l'ensemble des activités de cyberdéfense militaire pour l'année 2021. Contrairement à d'autres États, la cybersécurité interne des États-Unis (défense de son cyberespace et de ses réseaux, cybercriminalité, cyberterrorisme, etc.) n'est pas une compétence relevant du département de la Défense, mais bien du département de la Sécurité intérieure des États-Unis. (Homeland Security Department) Pour l'année fiscale 2021, un budget de presque 2,6 milliards de dollars ont été alloués pour ce type d'opérations de cybersécurité relevant du Département de la Sécurité intérieure des États-Unis et de son agence interne spécialisée en cybersécurité, le Cybersecurity and Infrastructure Security Agency (CISA)[28]. Leurs cyber unités sont impliquées surtout dans des projets de défense du cyberespace, déclarant officiellement que la Chine, la Russie, l'Iran et la Corée du Nord sont des menaces à la sécurité collective des membres dudit cyberespace américain[29]. Depuis les dix dernières années, ces cyber unités sont stationnées un peu partout à travers les États-Unis, en

[28] Statista. [s.d.] *Proposed federal spending by the U.S. government on cyber security for selected government agencies from FY 2020 to FY 2021*. Récupéré de : https://www.statista.com/statistics/737504/us-fed-gov-it-cyber-security-fy-budget/

[29] CISA. [s.d.] *Cybersecurity*. Récupéré de : https://www.cisa.gov/cybersecurity

Allemagne, au Koweït et en Corée du Nord, et ont participé à divers partenariats avec d'autres cyber unités à travers le monde.

Sur le plan militaire, le Canada est considéré comme une puissance dite moyenne par la communauté internationale. Toutefois, en matière de cybersécurité et de cyberdéfense, le Canada est très loin derrière des États comme les États-Unis, la France, le Royaume-Uni, la Russie et la Chine. En effet, le Canada est même critiqué tant à l'intérieur de ses institutions gouvernementales que sur la scène internationale pour son manque criant d'intérêt et de ressources humaines et matérielles en matière de cybersécurité et de cyberdéfense, et ce, même s'il a commencé à se doter d'outils en la matière en 2010, soit en même temps que ses voisins du Sud[30]. Il aura fallu attendre 8 ans - plus précisément, en octobre 2018 - et des milliards de dollars[31] pour qu'une stratégie un minimum concrète en matière de cyberdéfense et de cybersécurité soit développée par le gouvernement fédéral, confiant le gros des tâches et des projets à ce sujet au ministère des Affaires étrangères, au Centre de la Sécurité des Télécommunications (CST) et à la Gendarmerie royale canadienne (GRC) plutôt qu'aux Forces armées canadiennes[32]. Présentement, d'un point de vue offensif, les cyber unités de combat du Canada sont très peu actives sur la scène internationale. Étant donné le nombre considérables de cyberattaques orchestrées à l'égard des institutions gouvernementales canadiennes - on peut penser notamment aux cas récents des cyberattaques contre l'Agence du revenu du Canada[33] et de Service Canada à l'été 2020 - le gros des efforts canadiens en cyberdéfense et en cybersécurité sont concentrés dans une perspective défensive sur la protection des données de la population canadienne ainsi que de son cyberespace contre des menaces chinoises, russes, iraniennes et nord-coréennes[34]. Sur la scène internationale, le Canada participe à quelques initiatives intergouvernementales en matière de protection et d'encadrement du cyberespace, dont certaines d'entre elles en partenariat avec l'Organisation des Nations unies (ONU), l'Organisation du traité de l'Atlantique nord (OTAN) et

[30] Sécurité publique Canada. (2018) [s.d.] *National Cybersecurity Action Plan 2019-2024*. Récupéré de : https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf
[31] Ibidem.
[32] Gouvernement du Canada. [s.d.] *Un gouvernement juste et responsable*. Récupéré de : https://www.budget.gc.ca/2021/report-rapport/p4-fr.html
[33] Ibidem.
[34] Canadian Association of Defence and Security Industries. (2019) [s.d.] *2019 Annual Report - From Bullets to Bytes : Industry's role in preparing Canada for the future of Cyber Defence*. Récupéré de : https://www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-24.pdf

l'Organisation pour la sécurité et la coopération en Europe (OSCE) [35] portant sur la question du recours aux cyberarmes dans le cadre d'opérations stratégiques et militaires. Ces initiatives sont entre autres financées par le gouvernement canadien, qui y a investi plus de 13 millions de dollars depuis 2015[36]. En matière de budget, au cours de l'année fiscale 2019-2020, le Canada a investi 22,8 milliards dans sa défense nationale[37], dont 65,5 millions dans ses cyber opérations[38], ainsi que 126,5 millions dans un programme de développement des cyber unités de combats canadiennes[39]. Étrangement et curieusement, bien qu'il compte augmenter ses dépenses en matière de défense nationale d'un milliard de dollars d'ici la fin de l'année fiscale 2023-2024[40], le Canada compte couper dans ses investissements liés à ses cyber opérations et à ses cyber unités, leur accordant respectivement seulement 52,8 millions de dollars[41] et 102,1 millions de dollars[42] au cours de cette même période financière. Lorsqu'on compare ces investissements avec ceux d'autres pays occidentaux, il est à se demander quelle est la position réelle du Canada en matière de cyber opérations et de recours aux cyber armes.

Le cas de la Chine est plutôt particulier et intéressant à étudier, car bien qu'il s'agisse d'une des plus grandes puissances militaires cybernétiques sur la scène internationale, il n'y a que très peu d'informations à son sujet qui sont rendues disponibles pour le grand public. Selon le Centre d'excellence de cyberdéfense coopérative de l'OTAN (CCDCOE), la Chine aurait commencé graduellement à assembler plusieurs cyber unités offensives et défensives au sein des rangs de ses corps militaires dès 1997 et, en juillet 2010, aurait annoncé la création d'une « base de protection de l'information » au sein de l'Armée de libération du peuple (ALP) pour défendre ses réseaux informatiques et son cyberespace. (CCDCOE, 2013) Ces cyber unités sont identifiées non pas avec un nom en particulier - comme dans le cas des

[35]Gouvernement du Canada. [s.d.] *Politique internationale en matière de cyberespace*. Récupéré de : https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyber_policy-politique_cyberspace.aspx?lang=fra

[36]Ibidem.

[37]Gouvernement du Canada. [s.d.] *Infographie pour Défense nationale*. Récupéré de : https://www.tbs-sct.gc.ca/ems-sgd/edb-bdd/index-fra.html#orgs/dept/133/infograph/financial

[38]Gouvernement du Canada. [s.d.] *Infographie pour Cyberopérations*. Récupéré de : https://www.tbs-sct.gc.ca/ems-sgd/edb-bdd/index-fra.html#orgs/program/ND-BUN05/infograph/financial

[39]Gouvernement du Canada. [s.d.] *Infographie pour Cyberforces et systèmes de communication et d'information (SCI) interarmées prêts au combat*. Récupéré de : https://www.tbs-sct.gc.ca/ems-sgd/edb-bdd/index-fra.html#orgs/program/ND-BUO06/infograph/financial

[40]Gouvernement du Canada. [s.d.] *Infographie pour Défense nationale*. Récupéré de : https://www.tbs-sct.gc.ca/ems-sgd/edb-bdd/index-fra.html#orgs/dept/133/infograph/financial

[41]Gouvernement du Canada. [s.d.] *Infographie pour Cyberopérations*. Récupéré de : https://www.tbs-sct.gc.ca/ems-sgd/edb-bdd/index-fra.html#orgs/program/ND-BUN05/infograph/financial

[42]Gouvernement du Canada. [s.d.] *Infographie pour Cyberforces et systèmes de communication et d'information (SCI) interarmées prêts au combat*. Récupéré de : https://www.tbs-sct.gc.ca/ems-sgd/edb-bdd/index-fra.html#orgs/program/ND-BUO06/infograph/financial

États-Unis -, mais plutôt avec une série de lettres et de chiffres correspondant aux différents projets auxquels ces unités sont affiliées. Par exemple, l'une des cyber unités de l'ALP qui a été découverte par la communauté internationale est l'Unité 61486, qui serait, depuis 2007, l'une des cyber unités chinoises les plus actives en matière de cyberattaques contre des entreprises et des institutions occidentales[43]. En matière de budget, la Chine a établi au printemps 2021 un budget militaire annuel de 1,355 trillions de yuan chinois, ce qui équivaut à environ 270 milliards de dollars canadiens. Toutefois, aucun chiffre précis n'a été dévoilé en ce qui a trait aux dépenses liées aux activités de cyberdéfense, de cybersécurité et de cyberarmes. Cela dit, il a été récemment compris et analysé par des experts en géopolitique chinoise du International Institute for Strategic Studies (IISS) que l'ALP fait déjà d'énormes efforts de réformes en vue d'une modernisation et d'une numérisation complète de certains de ses corps internes d'ici quelques années, mettant l'accent sur la recherche et le développement d'armes et d'appareils intelligents[44]. Les experts de l'IISS ont également souligné dans leur analyse les ambitions de l'ALP pour remettre au goût du jour leur philosophie et leur approche en matière de théorie militaire, de vision du personnel, de leur organisation et de la relation entre le militaire et les civils[45]. En ce qui a trait à son implication sur la scène internationale, bien qu'elle ne revendique que très rarement les cyberattaques dont elle est l'auteure, la Chine est extrêmement active tant sur les plans offensifs que défensif à travers le monde, menant annuellement des dizaines de cyberattaques contre des institutions gouvernementales, pour la majorité des institutions occidentales. Par exemple, depuis 2006, l'Unité 61398 de l'ALP serait responsable de plus de 115 cyberattaques contre des entreprises américaines qui avaient pour but de voler et d'exposer leurs secrets commerciaux au reste du monde[46].

Le cas de la Russie est extrêmement similaire à celui de la Chine, étant donné que malgré qu'elle soit également une puissance cybernétique sur la scène internationale avec une grande réputation qui la précède, la Russie se fait extrêmement discrète en matière de partage

[43]Institute for Strategic Studies. [s.d.] *China's new Five-Year Plan and 2021 budget: what do they mean for defence?*. Récupéré de : https://www.iiss.org/blogs/analysis/2021/03/chinas-new-five-year-plan-and-2021-budget

[44] Shen, M. (2019, 29 juin) *China's Cyber Warfare Strategy and Approaches toward Taiwan*. Récupéré de : https://www.pf.org.tw/files/6510/A73CE07D-0D72-4AF8-9075-98A1CB188DA1

[45] Institute for Strategic Studies. [s.d.] *China's new Five-Year Plan and 2021 budget: what do they mean for defence?*. Récupéré de : https://www.iiss.org/blogs/analysis/2021/03/chinas-new-five-year-plan-and-2021-budget

[46] Shen, M. (2019, 29 juin) *China's Cyber Warfare Strategy and Approaches toward Taiwan*. Récupéré de : https://www.pf.org.tw/files/6510/A73CE07D-0D72-4AF8-9075-98A1CB188DA1

d'informations sur ses opérations qui ont lieu dans le cyberespace et ne revendique que très rarement les cyberattaques dont elle est responsable, comme dans les cas des cyberattaques qu'elle a menées contre l'Estonie en 2007 et contre la Géorgie en 2008. L'OTAN relate d'ailleurs ces derniers événements en Géorgie comme suit :

> The cyber attacks launched against Georgia during hostilities with Russia in August 2008 exemplify the potential of this new form of warfare. The Russian invasion of Georgia was preceded by cyber attacks consisting of website defacements and distributed denial-of-service (DDoS) attacks targeting government, news media, and financial websites. These attacks limited the Georgian government's ability to coordinate a response to the Russians and prevented Georgia from getting their story to the rest of the world. Whether these cyber attacks were coordinated by the Russian government or not, they were of benefit to Russia's subsequent invasion[47].

Bien qu'il soit difficile de dire exactement combien de cyberattaques sont commises par la Russie, on estime que celle-ci orchestre régulièrement et annuellement des dizaines de cyberattaques contre des particuliers et contre des institutions gouvernementales dans le but d'acquérir de l'intelligence et des données sur d'autres États à diverses fins stratégiques. « Cela inclut l'ingérence du GRU dans les élections parlementaires de 2020 en Géorgie, de même que la cyberépidémie NotPetya qui a causé, en 2017 des dommages massifs aux réseaux gouvernementaux et commerciaux, principalement en Ukraine.[48] » (Affaires mondiales Canada, 2020) Côté budget, la Russie aurait investi, en 2020, 61.7 milliards de dollars américains dans son budget militaire[49], mais, tout comme dans le cas de la Chine, l'information à savoir comment ce montant a été réparti entre les divers corps militaires - dont ses cyber unités offensives et défensives - n'est malheureusement pas disponible.

2.2. Conséquences réelles et potentielles du recours aux cyberarmes : rapports de force, dommages collatéraux et dommages intentionnels

Dans le cadre d'armes traditionnelles et de conflits armés, la grande majorité des dommages collatéraux d'une frappe sont visuellement faciles à estimer, à évaluer et à rapporter à l'organisation ayant orchestré ladite attaque : comme on connaît bien depuis

---

[47]NATO Cooperative Cyber Defence Centre of Excellence. [s.d.] *A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons*. Récupéré de : https://ccdcoe.org/uploads/2018/10/8_d1r2s6_raymond.pdf

[48] Affaires mondiales Canada. [s.d.] *Le Canada exprime son inquiétude face aux activités malveillantes des services de renseignements militaires russes*. Récupéré de : https://www.canada.ca/fr/affaires-mondiales/nouvelles/2020/10/le-canada-exprime-son-inquietude-face-aux-activites-malveillantes-des-services-de-renseignements-militaires-russes.html

[49]Statista. [s.d.] *Countries with the highest military spending worldwide in 2020*. Récupéré de : https://www.statista.com/statistics/262742/countries-with-the-highest-military-spending/

plusieurs années le potentiel des différentes armes qui constituent notre arsenal, on peut, par exemple, calculer d'avance le périmètre touché par la frappe, le nombre de morts et/ou de blessés touchés par cette frappe, les infrastructures et les ressources qui peuvent être endommagées et/ou menacées par une action en particulier, etc., en fonction de ou des armes choisies. Toutefois, dans le cadre des cyberattaques, pour les personnes et les dirigeants politiques qui sont moins familiers avec les cyberattaques et les outils informatiques en général, il est encore parfois difficile d'imaginer et d'évaluer les conséquences potentielles et réelles du recours aux cyberarmes. C'est entre autres pour cette raison que ces dommages collatéraux en question sont souvent sous-estimés par ces dirigeants politiques responsables de leur encadrement (voire carrément écartés de la question) et que ces derniers peuvent prendre des actions quelque peu douteuses en matière de cyberdéfense et de cybersécurité. Le CCDCOE estime que puisque les cyber opérations deviennent de plus en plus du ressort des chefs militaires en termes de logistique et de stratégie, il est primordial que les limites du comportement moral et éthique pour le déploiement des cyberarmes soient clairement encadrées et définies par le droit international humanitaire, en incluant tout ce qui a trait aux dommages collatéraux possibles, et que les États qui choisissent consciemment de ne pas adhérer à ces normes-là soient sévèrement sanctionnés par la communauté internationale[50]. La prochaine section étudiera les principales conséquences liées au recours des cyberarmes, à savoir les dommages collatéraux pour la population civile et pour leurs institutions ainsi que les changements dans les rapports de domination que leur utilisation peut engendrer.

Tout d'abord, l'une des conséquences réelles en lien avec le recours aux cyberarmes qui risque potentiellement de s'empirer avec le temps est l'ampleur des dommages intentionnels et collatéraux touchant directement la population civile et les institutions étatiques qui ont été visées par des cyberattaques. Le Comité international de la Croix-Rouge définit, dans son glossaire du droit international humanitaire, les dommages collatéraux comme des « dommages, pertes ou blessures causés accidentellement à des civils ou à des biens de caractère civil lors d'une attaque lancée contre un objectif militaire légitime, alors que toutes les précautions nécessaires avaient été prises pour prévenir ou limiter autant que possible ces dommages, pertes ou blessures. » (Comité de la Croix-Rouge, 2009) Tel que mentionné dans le premier chapitre, le droit international humanitaire actuel prévoit, via les

[50] NATO Cooperative Cyber Defence Centre of Excellence. [s.d.] *A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons*. Récupéré de : https://ccdcoe.org/uploads/2018/10/8_d1r2s6_raymond.pdf

Conventions de Genève, qu'aucune frappe militaire ne touche directement la population civile innocente - c'est-à-dire celle qui ne participe pas, de près ou de loin, aux violences d'un conflit armé - ni les installations qui sont cruciales à la survie de cette population, comme les installations médicales (cliniques et hôpitaux), les réserves d'eau potable, les réserves alimentaires agricoles, les moyens de transports civils (trains, autobus, avions commerciaux, etc.) et les habitations hors des bases militaires[51]. Ce même droit international humanitaire stipule que toute opération militaire conduite sans discrimination et sans prise de considération pour la population civile (surtout lorsque celle-ci est délibérément la cible des attaques perpétrées par des corps militaires) est proscrite, et que le fait de prendre délibérément des civils pour cible constitue un crime de guerre[52]. Dans un même ordre d'idées, le CICR rappelle qu'en vertu du droit international humanitaire et du principe de proportionnalité, s'il existe la moindre probabilité qu'une attaque cause des dommages collatéraux excessifs à l'égard de la population civile par rapport à l'avantage militaire concret et direct attendu, cette frappe militaire, de quelque façon dont elle se concrétise, doit être annulée ou interrompue[53].

Or, tel qu'il a été étudié plus tôt au cours de cette réflexion, contrairement aux frappes traditionnelles, il est presque impossible, dans le cas de cyberattaques militaires et de recours aux cyberarmes, de ne pas commettre de dommages directs contre la population civile innocente et il est extrêmement difficile de trancher sur la question de la proportionnalité pour se questionner si oui ou non il peut possible d'annuler ou d'interrompre ladite cyber opération en cours. En effet, lorsque des instances judiciaires se saisissent de cas de violences de guerres, ces instances prennent entre autres leur décision en fonction des dommages physiques qui sont causés par une opération militaire - le nombre de morts, de blessés, de bâtiments détruits, la quantité d'autres dommages matériels causés, le capital financier et humain nécessaires pour réparer ces dommages, etc. - pour juger si oui ou non cette frappe n'était pas conforme au droit international humanitaire. Dans le cas de cyber opérations, les dommages causés par l'État attaquant ne sont pas nécessairement tangibles, physiques, ce qui crée un énorme vide juridique pour déterminer si les dégâts causés par une cyberattaque peuvent être considérés d'abord comme un acte de guerre, mais également comme des dommages collatéraux. Romanosky et Goldman expliquent que les effets et les dommages

[51]Comité international de la Croix-Rouge. [s.d.] *Conduite des hostilités et droit international humanitaire*. Récupéré de : https://www.icrc.org/fr/document/conduite-des-hostilites
[52] Ibidem.
[53]Ibidem.

collatéraux issus d'une cyberattaque sont extrêmement différents de ceux causés, par exemple, par une frappe militaire traditionnelle, notamment parce que les cyberattaques causent essentiellement des dommages intangibles aux cibles touchées, comme une atteinte à la confidentialité, à l'intégralité et/ou à la disponibilité des données enregistrées sur un serveur touché par l'attaque[54]. Ils soulignent également que contrairement aux frappes traditionnelles, dans le cas d'une cyber opération, il est difficile d'évaluer d'avance les potentiels dommages causés par une cyberattaque tant au moment où l'attaque est lancée que dans les jours et les semaines suivant l'attaque en raison notamment de l'origine des dégâts causés et des failles de sécurité présentes antérieurement à l'attaque en question[55]. Ils synthétisent les débats autour de l'évaluation et de la reconnaissance des dommages collatéraux de cyberattaques ainsi :

> Harms that originate in code may be latent or transient. They may rely on the confluence of a number of different events to achieve their peak damage. Failures in technical systems may emerge for reasons that have nothing to do with code that is deliberately introduced. […] Indeed, a critical observation [...] is to demonstrate the ways in which evolving notions of harm in the cyber domain lack a comfortable place in the traditional context of collateral damage. For instance, consider a software vulnerability exploited by an adversary. The vulnerability is used to install a software program that causes the adversary's power station to overload and be physically destroyed. In this case, the method of committing the attack (i.e. using computer software to destroy the power station) should be irrelevant for the discussion of damage assessment[56].

Pire encore, dans la très grande majorité des cyber opérations, l'État attaquant prend nécessairement en otage la population civile innocente - en tout ou en partie - de ou des États visés par l'attaque ainsi que certaines de leurs institutions qui sont nécessaires au bon fonctionnement et à la survie de ladite population civile susmentionnée. Tel fut le cas de l'attaque des États-Unis et d'Israël contre les installations nucléaires iraniennes via le malware Stuxnet, qui a non seulement mis à terre plusieurs installations civiles iraniennes en tout genre (écoles, hôpitaux, commerces, etc.) en coupant leur alimentation en électricité issue des centrales nucléaires touchées, mais qui a aussi infecté des milliers d'ordinateurs qui n'étaient pas du tout visés par l'attaque au départ :

> Although this worm worked only with this specific software, it infected thousands of computers. A lot of lawyers and researchers wondered about the ethics of this kind of attacks: "at face value, Stuxnet seems

---

[54] Romanosky, S., et Goldman, Z. (2017, 6 octobre) Understanding Cyber Collateral Dammage. In *Journal of National Security Law and Policy*, 9 (2). https://jnslp.com/2017/10/06/understanding-cyber-collateral-damage/
[55] Ibidem.
[56] Ibidem.

> incredibly indiscriminant. While limited in the scope of its attacks compared to prior malware, this was a worm that still got around. It infected not just targets in Iran but thousands of computers across the world that had nothing to do with Iran or nuclear research. Many lawyers see this facet of cyber weapons as proof of their inherent violation of "prevailing codes of international laws of conflict, as they go beyond just the original target and deliberately target civilian personnel and infrastructure[57]."

À l'heure actuelle, il est de plus en plus inquiétant de constater qu'aucune action n'ait été entreprise ni pour traduire en justice ce type d'attaque - qui est clairement une violation du droit international humanitaire - ni pour reconnaître les dommages collatéraux et intentionnels venant du recours aux cyberarmes. Une reconnaissance étatique, politique et juridique des types de dommages possibles dans le cyberespace est donc plus que jamais nécessaire.

Ensuite, l'une des conséquences potentielles en lien avec le recours aux cyberarmes qui est déjà possible d'observer est un changement dans les rapports de force militaires sur la scène internationale. En effet, bien qu'à l'heure actuelle, la Chine et les États-Unis soient les deux plus grandes puissances militaires tant dans le cadre de combats traditionnels que dans le cyberespace, et que la Russie est un acteur détenant un rôle-clé également dans les actions menées dans le cyberespace, force est de constater que l'avènement du recours aux cyberarmes dans le cadre d'opérations stratégiques et militaires donne énormément d'avantages à des joueurs qui ne se sont pas vraiment démarqués sur la scène militaire internationale dans le cadre de combats traditionnels et/ou qui ne sont pas nécessairement reconnus comme des superpuissances militaires. Par exemple, l'Iran, le Pakistan, l'Inde, la Suède et le Japon ne sont pas traditionnellement forcément reconnus comme des grandes puissances militaires sur la scène internationale, mais ils sont toutefois des États très importants qui se démarquent de plus en plus dans le cadre d'opérations menées dans le cyberespace. Comme l'expliquent Friedman et Signer ainsi que d'autres experts en matière de combats cybernétiques, ce qui définit un acteur important et puissant dans le cyberespace est, certes, sa capacité à se défendre contre de potentielles cyberattaques - notamment en démontrant à quel point leur cybersécurité et leurs stratégies de cyberdéfense sont bien développées - , mais c'est surtout la capacité à mener une cyber opération offensive avec succès qui le fera: dans le cadre d'une opération militaire traditionnelle, les étapes de préparation d'une frappe et d'un combat sont certes fastidieuses, mais nécessitent beaucoup moins d'étapes et de reconnaissance du terrain qu'une cyberattaque. En effet, dans le cadre

[57] Artese, E. et Vitkov, V. (2015, novembre) Cyberwarfare and Collateral Damages. In *Globalex*. Récupéré de: https://www.nyulawglobal.org/globalex/Cyberwarfare_Collateral_Damages.html

d'une cyberattaque, un cyberattaquant doit nécessairement réussir à outrepasser au préalable - sans se faire remarquer par l'État visé par la future cyberattaque - toutes les barrières de sécurité mises en place dans le cadre de protocole de cybersécurité pour s'infiltrer dans les systèmes informatiques qu'il compte frapper et étudier toutes les moindres failles de sécurité présentes dans ces systèmes informatiques pour les exploiter dans son attaque plus tard, un chemin à frayer qui s'appelle un «cyber kill chain». « The attacker has to take a number of steps: reconnaissance, build a weapon, deliver that weapon, pull information out of the network. Each step creates a vulnerability, and all have to be completed. But a defender can stop the attack at any step [of it]. » (Signer et Friedman, 2014, p.155) Le tout a beau coûter moins cher à planifier et à préparer qu'une reconnaissance de terrain via images satellites, mais ce processus est néanmoins beaucoup plus complexe et plus long à faire. Seul un acteur capable à la fois de démontrer à plusieurs reprises qu'il est en mesure de se frayer un chemin à travers un «cyber kill chain» sans se faire intercepter et de démontrer qu'il a effectivement l'arsenal nécessaire pour défendre adéquatement tous les recoins de son cyberespace peut être véritablement considéré comme une puissance militaire cybernétique[58].

2.3. Cyberattaques étatiques importantes

Afin de mieux comprendre la magnitude des enjeux de sécurité en lien avec l'usage de cyberarmes, il est important d'étudier des cas de figure classiques et particuliers de cyberattaques étatiques qui hantent encore l'imaginaire collectif du politique et du génie informatique. Dans le cas de la présente réflexion, le cas des cyberattaques russes contre le gouvernement estonien en 2007 et l'opération israélo-américaine Olympic Games contre l'Iran seront étudiés afin de comprendre ce qui s'est passé, quelles cyber armes ont été utilisées, quels dégâts ont été causés et quels en sont des dommages collatéraux ou les débouchées de ces événements cybernétiques.

Au printemps 2007, l'Estonie était perçue comme un précurseur sur la scène internationale en matière de numérisation des services étatiques et privés offerts aux citoyens : déjà à l'époque, presque tous ses citoyens avaient une identité numérique qui leur donnait accès à divers services financiers, éducatifs et socio-sanitaires à travers le pays, comme les banques, les institutions scolaires de tous les niveaux, les bibliothèques, les services gouvernementaux provenant de différents ministères, les soins de santé, etc. Cette identité

[58] Singer, P.W., et Friedman, A. (2014) *Cybersecurity and Cyberwar: What everyone needs to know*, New York, Oxford University Press, 2014. (p.154-155)

numérique leur permettait également d'avoir accès à un fournisseur d'Internet, aux différents médias estoniens, aux plateformes d'achats en ligne de plusieurs commerces, etc. Peu de temps avant la série de cyberattaques, après que le gouvernement estonien ait annoncé que la statue du Mémorial du Soldat de Bronze[59] sera déplacée du centre de la ville vers un cimetière aux limites de celle-ci, les tensions entre l'Estonie et les Russes ont escaladé, et de nombreuses révoltes et manifestations anti-Ansip (nom du premier ministre estonien de l'époque) se sont tenues un peu partout tant du côté estonien que du côté russe. De la fin avril à la mi-mai 2007, pendant trois semaines, une série d'attaques de type DDOS (Distributed Denial of Service) ont paralysé tous les services numériques de l'Estonie, figeant du même coup l'ensemble des activités quotidiennes et économiques du pays. Résultats : la population estonienne ne pouvait plus avoir accès à de l'information, à leurs comptes bancaires, à leurs services publics, et plus encore[60]. Bien qu'encore aujourd'hui, presque quinze ans après les faits, le gouvernement russe n'ait toujours pas officiellement affirmé qu'il était le responsable de ces cyberattaques contre les institutions estoniennes, plusieurs preuves accumulées au fil des ans le pointent du doigt, dont des déclarations faites par des officiels russes et des adresses IP desquelles étaient originaires certains botnets utilisés lors de quelques-unes des cyberattaques de types DDOS en question au cours de cette période.

> The vast majority of malicious network traffic was of Russian-language origin and had indications of political motivation. The Russian government denied any involvement; however, the cyber attacks were accompanied by hostile political rhetoric by Russian officials, unfriendly economic measures, and refusal to cooperate with the Estonian investigation in the aftermath of the attacks, all of which likely encouraged the perpetrators[61].

Dans les mois qui ont suivi ces cyberattaques, le même modus operandi (avec encore une fois des serveurs et des adresses IP russes) a pu être observé dans le cadre de cyberattaques menées contre la Lituanie et la Géorgie en 2008 ainsi que contre le Kyrgyzstan en 2009 après une montée des tensions entre ces États mentionnés et la Russie[62]. Il est toutefois possible de dire que les cyberattaques contre de l'Estonie ont été l'élément déclencheur d'une série de discussions et de réflexions sur la scène internationale en matière de cybersécurité, d'adoption de mesures et de lois nationales en matière de cyberdéfense et de cybersécurité, de recours

[59]Le Mémorial du Soldat de Bronze est statue au centre de Tallinn, la capitale estonienne, offerte par les Soviétiques à l'Estonie après la Seconde Guerre mondiale et symbolisant la libération du territoire estonien par l'URSS de l'emprise de l'Allemagne nazie.

[60]Artese, E. et Vitkov, V. (2015, novembre) Cyberwarfare and Collateral Damages. In *Globalex*. Récupéré de: https://www.nyulawglobal.org/globalex/Cyberwarfare_Collateral_Damages.html

[61]NATO Strategic Communications Center of Excellence. [s.d.] *Hybrid Threats: 2007 cyber attacks on Estonia*. Récupéré de : https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86

[62]Ibidem.

aux cyberarmes, de l'avenir des conflits cybernétiques, et plus encore, dont le *Tallinn Manual*[63], un document célèbre créé par un groupe d'experts politiques, juridiques et militaires en cyberdéfense qui permet d'expliquer comment le droit international humanitaire actuel s'applique au recours aux cyberarmes.

Une série de cyberattaques encore plus mythique dans l'imaginaire collectif des militaires et des spécialistes en informatique et en cybersécurité est l'opération Olympic Games menée par les États-Unis et Israël contre de l'Iran entre 2006 et 2011, qui a particulièrement choqué la communauté internationale par la puissance de la cyberarme Stuxnet, par les intentions derrières l'attaque et par les multiples violations du droit international humanitaire commises dans le cadre de cette cyber opération. Stuxnet est un malware dont le code cible des vulnérabilités en particulier qui sont le résultat d'une combinaison de systèmes d'exploitation en particulier et de logiciels présents sur un appareil ; si cette combinaison n'est pas présente, Stuxnet reste dormant et invisible sur l'appareil infecté jusqu'à ce que cette combinaison soit présente sur l'appareil[64]. Cette combinaison était particulièrement présente dans une série de centrifugeuses nucléaires d'un certain âge qui, « par le plus grand des hasards », étaient à la centrale nucléaire de Natanz, en Iran, une centrale dont la communauté internationale suspectait la présence d'armes nucléaires illicites[65]. Pour endommager les systèmes infectés, Stuxnet utilise plusieurs techniques différentes de cyberattaques, dont la zero day et la MITM. Il a été créé et développé entre 2006 et 2009 par les Américains et les Israéliens dans le but de neutraliser le site de Natanz. Pendant plus d'un an, personne parmi les employés de Natanz n'a remarqué qu'un virus informatique s'était infiltré dans les systèmes informatiques de la centrale tant celui-ci était discret et efficace : les bris, les explosions et les pannes de centrifugeuses causées par la présence de Stuxnet était souvent attribuée à un mauvais entretien de la centrale par les ingénieurs qui y travaillaient[66]. Stuxnet a tellement été dévastateur pour l'Iran et sa population - ainsi que pour les autres ordinateurs à travers le monde touchés par cette cyberattaque - que dix ans plus tard, celle-ci commence tout juste à se remettre des effets catastrophiques de cette cyberattaque. Bien que Stuxnet soit maintenant encore une référence lorsque des experts et des dirigeants discutent de recours aux cyberarmes et de leurs effets, aucune convention internationale ni amendement au

[63] NATO Strategic Communications Center of Excellence. [s.d.] *Hybrid Threats: 2007 cyber attacks on Estonia*. Récupéré de : https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86
[64] Singer, P.W., et Friedman, A. (2014) *Cybersecurity and Cyberwar: What everyone needs to know*, New York, Oxford University Press, 2014. (p.116)
[65] Ibidem.
[66] Ibidem.

droit international humanitaire n'a été adopté depuis ces incidents pour mieux encadrer l'usage de cyberarmes dans le cadre d'opérations stratégiques et militaires.

Que ce soit dans le cas de l'Estonie ou de Stuxnet, il est important de se rappeler qu'aucune arrestation ni condamnation n'a été faite pour punir les personnes responsables de ces attaques en vertu du droit international humanitaire en vigueur, et ce, bien que la communauté internationale se soit largement exprimée en défaveur de telles cyberattaques étatiques. Ces cyberattaques classiques, comme d'autres cyberattaques qui ont été exécutées depuis, auraient été de très bonnes opportunités pour les cours internationales de justice de créer la jurisprudence adéquate pour renforcer et appliquer le droit international humanitaire ainsi que pour traduire en justice ceux qui se permettent d'agir contre celui-ci.

2.4. Recommandations politiques d'améliorations en matière de traitement d'enjeux de cybersécurité

Maintenant que les enjeux politiques de sécurité autour du recours aux cyberarmes aient été étudiés - notamment en analysant qui sont quatre des principaux acteurs et quelles en sont les conséquences réelles et potentielles, entre autres via l'étude de deux cas de figure classiques -, des recommandations en matière de traitement et de résolution de ces enjeux sont de mise. À la lueur de la littérature existante, la présente partie de cette réflexion portera sur deux recommandations qu'il serait possible de faire aux dirigeants politiques de la scène internationale pour éventuellement résorber lesdits enjeux politiques de sécurité dont il a été question plus tôt au cours de cette réflexion.

La toute première recommandation à faire pour améliorer le traitement d'enjeux politiques de sécurité liés à l'usage de cyberarmes est d'éduquer les dirigeants politiques sur les questions de cybersécurité afin qu'ils comprennent ce dont il est question lorsque ce sujet est abordé et ainsi que l'ampleur des conséquences de leurs décisions qui s'y attachent. En effet, comme en discutent Signer et Friedman dans leur ouvrage, la très grande majorité des dirigeants politiques - le problème étant encore plus criant au niveau des dirigeants occidentaux - ne sont pas du tout familiers avec des notions de base d'informatique et de cybersécurité, si bien qu'un écart important en termes de communications et transmission des savoirs s'est creusé entre la classe politique et les fonctionnaires issus des services informatiques des différents services gouvernementaux. Signer et Friedman traitent de ce manque de connaissances informatiques au sein de la classe politique ainsi :

> [...] The world is still mostly led by ‘’digital immigrants’’, older generations for whom computers and all the issues the Internet age presents remain unnatural and often confusing. [...] Cybersecurity is one of those areas that has been left to only the most technically inclined to worry their uncombed heads over. Anything related to the digital world of zeros and ones was an issue just for the computer scientists and the IT help desk. Whenever they spoke, most of us would keep quiet, nod our heads, and put on what author Mark Bowden calls ‘’the glaze’’. This is the ‘’unmistakable look of profound confusion and disinterest that takes hold whenever conversation turns to workings of a computer.’’ The glaze is the face you put on when you can only call something ‘’stuff’’. Similarly, those who are technically inclined too often roll their eyes at the foreign logic of the policy and business worlds, scoffing at the ‘’old way’’ of doing business, without understanding the interactions between technology and people. The result is that cybersecurity falls into a no man’s land. The field is becoming crucial to areas as intimate as your privacy and as weighty as the future of politics. But it is a domain only well known by ‘’the IT Crowd’’. It touches every major area of public - and private - sector concern, but only because the young and the computer savvy are well engaged with it. [...] This gap has wide implications. One US general described to us how ‘’understanding cyber is now a command responsibility’’, as it affects almost every part of modern war. [...] International relations are already becoming poisoned by this disconnect between what is understood and what is known[67].

Sans nécessairement que chaque politicien ait fait de grandes études supérieures en informatique ou en cybersécurité pour pouvoir occuper un haut poste bureaucratique au sein d’un gouvernement, il est tout de même crucial qu’une formation de base en cybersécurité qui va plus loin que celle fournie présentement aux employés de la fonction publique, c’est-à-dire celle qui ne contient que quelques éléments de gros bon sens tels que «ne pas avoir le même mot de passe - 123abc, le nom de son partenaire de vie, sa date de naissance, etc. - pour tous ses accès informatiques» ou «ne pas cliquer sur un fichier ou sur un lien dans courriel qui vous semble suspect», soit donnée aux dirigeants politiques pour qu’ils puissent prendre des décisions éclairées en matière de recours aux cyberarmes. Il est crucial également qu’un terrain d’entente soit trouvé entre les experts en cybersécurité recrutés par le gouvernement et la classe politique pour vulgariser adéquatement l’information en matière de cybersécurité et de cyberarmes pour la rendre plus accessible aux plus novices sans trop en compromettre la qualité desdites informations. Ainsi, l’écart de connaissances dont il était question ci-haut sera moins grand et il sera peut-être possible de faire avancer les choses plus efficacement dans l’avenir si cet effort de coopération est fait.

---

[67]Singer, P.W., et Friedman, A. (2014) *Cybersecurity and Cyberwar: What everyone needs to know*, New York, Oxford University Press, 2014. (p.5-6)

Allant dans un sens similaire à la première recommandation ci-haut, la seconde recommandation à faire pour améliorer le traitement d'enjeux politiques de sécurité liés à l'usage de cyberarmes est d'encourager les dirigeants politiques à investir davantage dans la recherche et le développement de leurs cyber forces armées pour les améliorer et pouvoir se préparer en cas de cyberattaque majeure surprise, histoire d'éviter de répéter la même histoire qu'en Estonie en 2007 ou celle de Stuxnet dont il a été question plus tôt. De plus en plus de dirigeants politiques s'en rendent compte, prennent position à ce sujet et emboîtent le pas à d'autres pour montrer l'exemple, comme dans le cas du ministère des Armées de la France :

> Face à la multiplication récente des cyberattaques, ainsi qu'à leur gravité, le ministère des Armées a revu à la hausse ses objectifs de recrutement dans la cyberdéfense. Il prévoit d'embaucher « 770 cybers combattants en plus des 1 100 initialement prévus » d'ici à 2025 [...]. Or « compte tenu de la multiplication et de la gravité des cyberattaques, j'ai décidé d'intensifier les recrutements » [...] « Le ministère des Armées a des missions et des enjeux […] qui nécessitent que nous utilisions l'arme "cyber" en appui de nos opérations. Nos adversaires ne s'en privent pas, qu'ils s'agissent de puissances étatiques, de groupes terroristes ou de leurs soutiens. » [...] L'annonce de ces recrutements supplémentaires au sein de la cyberdéfense « démontre une prise de conscience de la vulnérabilité de plus en plus importante de nos sociétés » face au risque d'attaques dans ce domaine « et du besoin d'y faire face et d'agir » [...]. La France veut montrer « qu'elle est là, qu'elle a des moyens et qu'elle défendra ses intérêts stratégiques ». La question est maintenant de savoir où vont « aller les recrutements, vers le défensif ou vers l'offensif » [...][68].

En effet, plusieurs États occidentaux qui sont historiquement considérés comme des puissances moyennes ou des grandes puissances sur les plans militaires n'investissent qu'une infime partie de leur budget militaire dans le développement de leurs cyber forces, si bien que celles-ci sont quasi-inexistantes et/ou ne pourraient pas compétitionner avec des (relativement) nouveaux joueurs sur la scène militaire internationale comme l'Inde[69], le Japon[70], la Chine et la Russie. Par exemple, l'Inde[71] et le Canada n'investissent que 0,8% de son budget militaire dans leurs cyber forces armées, contre 0,55% pour le Japon (30.1 milliards pour 5.34 trillions de yens) 1,4% pour les États-Unis et 4% pour la France. Il est

---

[68]Le Monde avec AFP. (2021, 8 septembre) Cybersécurité : la défense française veut renforcer ses troupes de cybercombattants.In *Le Monde*.Récupéré de: https://www.lemonde.fr/pixels/article/2021/09/08/cybersecurite-la-defense-francaise-etoffe-ses-troupes-de-cybercombattants_6093949_4408996.html

[69]Statista. [s.d.] *Value of expenditure towards cyber security in India in 2019 with a forecast for 2022, by sector*. Récupéré de : https://www.statista.com/statistics/1099728/india-expenditure-towards-cyber-security-by-sector/

[70]Ministère de la Défense du Japon. (2021) *Defense Programs and Budget of Japan - Overview of FY2021 Budget* [Rapport budgétaire annuel] https://www.mod.go.jp/en/d_act/d_budget/pdf/210331a.pdf

[71]Kaushik, K. (2021, 27 avril) India third highest military spender in 2020, states data published by Stockholm International Peace Research Institute. In *Indian Express*. Récupéré de : https://indianexpress.com/article/india/india-third-highest-military-spender-in-2020-7290118/

toutefois à noter que bien que nous n'ayions pas les chiffres pour la Chine et la Russie, et que les proportions pour l'Inde et le Japon semblent faibles, ces quatre États investissent depuis beaucoup plus longtemps dans leurs cyber unités et dans leur cybersécurité que la plupart des États occidentaux (France, Canada, États-Unis, etc.) ; on parle ici d'une avance d'au minimum 10 ans, voire 15 dans certains cas. Étant donné l'importance que prennent de plus en plus les cyber forces et les cyberarmes, il est donc nécessaire, pour rattraper ce retard technologique au sein des corps armés touchés, de faire les investissements nécessaires en matière de recherche et de développement sur ces plans.

Chapitre 3 Dimension juridique des enjeux autour de l'utilisation de matériel technologique à des fins stratégiques et militaires

3.1. Cadre juridique actuel

Après avoir étudié plusieurs aspects politiques de la question du recours aux cyberarmes par les États, il est maintenant temps d'analyser plus en profondeur les aspects juridiques de cette question. Pour ce faire, il est important d'identifier quels sont les principaux textes juridiques qui encadrent le recours aux cyberarmes dans le cadre d'opérations stratégiques et militaires et d'en étudier le contenu pour pouvoir éventuellement en souligner les limites et proposer des pistes d'amélioration. Bien que plusieurs organisations internationales aient adopté des résolutions pour appeler les États à mettre à jour le droit international pour que celui-ci puisse mieux encadrer ce qui se passe dans le cyberespace, et que des groupes d'experts juridiques tentent d'expliquer comment le droit international actuel répondrait déjà à ce type de besoins, le cadre juridique touchant le cyberespace et le recours aux cyber armes est, à l'heure actuelle, extrêmement limité et lacunaire. Ces lacunes sont notamment partiellement expliquées par la complexité et la nouveauté (d'un point de vue spatio-temporel) du phénomène du recours aux cyberarmes et de la cybersécurité en général. Cette partie de la réflexion se concentrera essentiellement sur la Convention de Budapest et sur les Conventions de Genève, qui sont les deux principaux textes juridiques à caractère contraignant - pour ne pas dire les deux seuls - qui touchent respectivement la cybersécurité et l'encadrement de conflits armés.

Tel que discuté dans le premier chapitre de cette réflexion, l'unique texte juridique de droit international public en vigueur qui a une portée contraignante pour ses États signataires et qui légifère sur la question de la cybersécurité et des cyberattaques est la Convention de Budapest du Conseil de l'Europe, qui a été adoptée en 2001, qui est entrée en vigueur en 2004. Cette convention a été déposée et adoptée alors que des dirigeants politiques du Conseil de l'Europe se sont rendu compte, à la fin des années 1990, que les outils informatiques étaient de plus en plus utilisés dans le cadre de crimes nationaux et internationaux tels que l'atteinte aux droits d'auteurs, la pédopornographie, la fraude informatique et le trafic ainsi que le vol de données stockées sur du matériel informatique à des fins illégales[72]. Depuis son entrée en vigueur en 2004, et surtout, depuis les événements en Estonie et en Iran, la Convention de Budapest a permis à plusieurs pays de se doter d'un cadre juridique en matière

[72] *Convention sur la cybercriminalité*, 2001, STE 185 –23.XI.2001 (entrée en vigueur le 1er juillet 2004) [Conseil de l'Europe]

de protection de leur cyberespace et de la cybersécurité tant de leurs institutions que de ceux de leurs concitoyens. Elle a également permis de lancer plusieurs initiatives et programmes intergouvernementaux en matière de cybersécurité internationale, de cyberdéfense, de recherche en la matière, et plus encore. Depuis le mois d'août 2021, cette convention internationale est en vigueur et intégrée au droit interne de 66 États des 193 États-membres de l'Organisation des Nations unies[73], dont la plupart sont également des États membres du Conseil de l'Europe. Pour environ le tiers de ces 66 États, le processus d'intégration de cette convention internationale à leur droit interne s'est finalisé au cours des cinq dernières années. Tel est le cas, par exemple, de la Suède, qui fait partie des premiers pays à avoir signé cette convention en 2001 et dont l'entrée en vigueur sur son territoire ne s'est officialisée que le 1er août 2021[74], soit plus de 20 ans après l'avoir signée, et de la Grèce, qui a signé cette convention au moment de son adoption et dont l'entrée en vigueur sur son territoire ne s'est officialisée que le 1er mai 2017[75].

Étant donné que son contenu n'a pas été mis à jour depuis son entrée en vigueur en 2004, la Convention de Budapest de 2001 comporte plusieurs limites juridiques. La première - et la plus évidente - est le fait que plusieurs des technologies et des techniques utilisées de nos jours pour mener à terme des cyber opérations et pour commettre des crimes - dont du cyber espionnage, du cyberterrorisme, de l'évasion fiscale, etc. - ne sont pas encadrés par cette convention parce qu'ils n'existaient pas au moment de la rédaction et de l'adoption de son texte. Le simple fait de mettre à jour son contenu permettrait de mieux encadrer le recours aux cyberarmes par les États dans le cadre de leurs opérations stratégiques et militaires ainsi que la cybersécurité internationale de manière générale. La deuxième limite est le fait que puisque la Convention de Budapest est issue du droit international public et non du droit international humanitaire, la majeure partie du contenu de cette convention internationale ne s'applique pas au cadre militaire et davantage à la cybercriminalité commise par des acteurs non-étatiques, comme des individus, des entreprises et des groupes issus du crime organisé. Si les États ne sont pas motivés à vouloir mettre à jour le contenu de la Convention de Budapest pour y intégrer du contenu qui permettrait d'encadrer les activités militaires qui ont lieu dans le cyberespace, il serait tout de même pertinent que ceux-ci discutent et finissent par carrément

[73]Council of Europe. [s.d.] *Chart of signatures and ratifications of Treaty 185*. Récupéré de : https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185
[74]Ibidem.
[75]Ibidem.

adopter une nouvelle convention internationale issue du droit humanitaire qui permettrait de légiférer sur la question du recours aux cyberarmes.

Les Conventions de Genève d'août 1949 et ses protocoles additionnels - qui ont été signés et adoptés entre 1977 et 2008 - sont les premiers textes juridiques du droit international humanitaire à porter sur les recours des États et de leur population civile en cas de conflits armés. Ces textes ont été rédigés et adoptés au lendemain de la Seconde Guerre mondiale pour interdire le recours à la force armée - ou du moins, mettre en place une multitude de mécanismes de règlement des différends pour les États qui fasse en sorte que le recours à la force armée soit l'ultime option restante une fois toutes les autres options épuisées - , proscrire le recours à certains types d'armes en particulier - et surtout, proscrire le recours à la force armée visant directement la population civile à des fins militaires -, réitérer l'importance du respect des droits humains de la population civile et définir d'importants concepts qui sont toujours utilisés aujourd'hui lorsqu'on étudie des conflits armés et le droit international humanitaire, comme les concepts de prisonniers de guerre et de crimes de guerre. Ces Conventions viennent compléter le texte de la Charte des Nations unies en matière de protection des individus dans le cadre de conflits armés et est appliquée par tous les États-membres de l'Organisation des Nations unies.

En matière de cyberdéfense, les Conventions de Genève et ses protocoles comportent plusieurs limites, et ce, même si ces limites font présentement l'objet d'importants débats au sein de la communauté internationale. La plus importante d'entre toutes - et qui est celle qui est au centre de tous les débats au sujet du cyberespace - est le fait qu'en principe, en lisant chaque article de chacune des conventions et de ses protocoles, les violences cybernétiques commises dans le cadre de cyber opérations militaires ne s'appliquent pas - ou très mal - au droit international humanitaire. En effet, peu importe que ce soit les principes d'agression, de dommages collatéraux et intentionnels, de recours à la force armée ou tout autre principe lié traditionnellement aux conflits armés, le droit international humanitaire actuel - et plus particulièrement les Conventions de Genève - ne reconnaissent pas le caractère intangible du cyberespace ainsi que les dommages virtuels causés par des cyberarmes dans le cadre de cyber opérations militaires : ces dommages, ces agressions et ces démonstrations de force armée doivent être physiquement observables pour que les Conventions de Genève puissent

s'appliquer[76]. On doit pouvoir voir et toucher, par exemple, des corps blessés ou inanimés, des immeubles embrasés et des ruines de villes bombardées pour que ces Conventions puissent s'appliquer et qu'on puisse dire avec certitude qu'il y a eu transgression du droit international humanitaire. Alors que des groupes comme le Comité international de la Croix-Rouge argumentent toutes les façons possibles dont le droit international humanitaire et les Conventions de Genève peuvent s'appliquer aux conflits cybernétiques, force est de constater, comme l'argumentent Singer et Friedman, que le phénomène des conflits cybernétiques est encore tellement nouveau que le cadre juridique les concernant ne semble pas évoluer au même rythme que ceux-ci. Ceux-ci argumentent que la majorité des règles du droit international humanitaire datent de la Seconde Guerre mondiale et qu'elles n'ont pas vraiment été remises au goût du jour depuis en raison de plus différences d'opinions entre les membres du système international, ce qui contribuerait à la désuétude du droit international en la matière, au manque de clarté quant à son application aux questions technologiques ainsi qu'à l'absence de la possibilité d'un conflit dont les effets et les frontières du territoire s'y déroulant seraient intangibles[77]. Ces auteurs appellent également les dirigeants politiques à appliquer certains principes de base du droit international humanitaire pour reconnaitre officiellement la violence des conflits ayant lieu dans le cyberespace comme solution temporaire en attendant de s'entendre sur un nouveau cadre juridique portant sur les questions cybernétiques[78].

> The problem is that this assumes only a physical world of clearly demarcated borders. […] cyberattacks don't use physical force, take place in a geographic realm, nor necessarily involve other states. [...]So until the old treaties are updated, or new ones are accepted for the cyber world, there is a third option: apply existing laws' basic principles and values to cyberspace. [...] ''A cyber attack is governed by basically the same rules as any other kind of attack.'' The primary way to determine when a cyberattack constitutes the kind of ''use of force'' that legally justifies war is to weigh its effects. What did the act do to the real world, regardless of the fact that it happened via cyber means? Look to the amount of damage, caused or intended, and establish parallels[79].

Il est donc plus que jamais crucial que les États-membres de l'ONU amendent les Conventions de Genève et ses protocoles pour pouvoir y incorporer tout ce qui a trait aux conflits cybernétiques et au recours aux cyberarmes.

---

[76] Singer, P.W., et Friedman, A. (2014) *Cybersecurity and Cyberwar: What everyone needs to know*, New York, Oxford University Press, 2014. (p.123-124)
[77] Ibidem.
[78] Ibidem.
[79] Ibidem.

Avant d'aller plus loin dans cette réflexion, il est important de noter que bien que le Tallinn Manual soit une référence depuis sa première parution en 2009 tant en relations internationales qu'en droit international en matière de recours aux cyberarmes et à l'encadrement de cyber opérations stratégiques et militaires, cet ouvrage de référence issu de l'initiative intergouvernementale des membres de l'OTAN n'a aucune portée juridique contraignante; il peut être utilisé par les civils pour créer de la littérature sur le sujet, mais il ne peut malheureusement pas être utilisé pour créer de la jurisprudence et pour accuser un État d'avoir enfreint le droit international humanitaire en menant une cyberattaque qui visait directement des institutions gouvernementales et qui mettait en péril l'intégrité des membres de la société civile de l'État touché par l'attaque. D'ailleurs, ayant remarqué à quel point le nombre de cyberattaques étatiques a explosé au cours des dernières années depuis la parution de la 2e édition du manuel et à quel point cette dernière est une référence importante utilisée par les différents juristes du droit international, une troisième édition revue et corrigée de ce manuel est présentement en cours de rédaction, et sa parution est prévue pour 2026[80].

3.2. Enjeux principaux liés au cadre juridique actuel

Afin d'étudier adéquatement les principaux enjeux juridiques entourant le choix de recourir aux cyberarmes dans le cadre d'opérations stratégiques et militaires, il est important d'identifier quels sont les principaux enjeux liés au cadre juridique actuel qui est lié audit recours en question. Étant donné le manque de coopération interétatique entre les différentes instances gouvernementales pour agir sur la question des cyberarmes au sein du système international, de nombreuses organisations internationales ont emboîté le pas aux États sur cette question pour les conseiller, mieux les outiller et les empresser d'agir. Cette partie de la réflexion se concentrera sur d'autres enjeux importants en lien avec le cadre juridique autour du cyberespace - autres que l'obsolescence de celui-ci et le manque de coopération internationale pour le mettre à jour et/ou l'améliorer - comme la personnalité juridique des organisations internationales et leur processus décisionnel prescrit par leur charte. Cette partie de cette réflexion expliquera également en quoi la personnalité juridique des organisations internationales ainsi que leur processus en matière d'adoption de décisions importantes - comme des documents à portée juridique - peuvent être un frein à un encadrement adéquat des

[80]Marks, J., et Schaffer, A. (2021, 21 juin) The Cybersecurity 202: Legal scholars are working on new rules for international hacking conflicts. *The Washington Post*. Récupéré de : https://www.washingtonpost.com/politics/2021/06/21/cybersecurity-202-legal-scholars-are-working-new-rules-international-hacking-conflicts/

cyberarmes et du cyberespace sur la scène internationale, le tout en étudiant plus précisément le cas de l'Organisation des Nations unies et de ses organes subsidiaires.

Le tout premier enjeu juridique lié aux organisations internationales qui les empêche de mieux agir sur la scène internationale en matière d'amélioration du droit international humanitaire et de recours aux cyberarmes est au cœur de leur personnalité juridique, qui leur confère des droits et des pouvoirs, mais qui les limite également. Les organisations internationales sont effectivement reconnues par le droit international public et le droit international humanitaire comme des personnes morales, ce qui leur confère un devoir et un pouvoir d'éducation, de sensibilisation, de suggestion et de recommandation auprès de ses membres. Dans la plupart des cas, les décisions prises par les organisations internationales, comme les motions et les résolutions, n'ont aucune portée contraignante pour ses États-membres, c'est-à-dire que l'administration de ces organisations internationales ne peut forcer les États-membres ni à accepter, ni à appliquer le contenu de ces décisions prises, ni leur appliquer des sanctions dans le cas où les États-membres ne reconnaîtraient pas ou agiraient contrairement au contenu desdites décisions. Par exemple, certains organes subsidiaires de l'ONU ont adopté, au fil des années, via l'Assemblée générale des Nations unies, des résolutions appelant les États à coopérer et à légiférer sur la question de la cybercriminalité, du cyberespionnage, du cyberterrorisme et de la sécurisation du cyberespace en général[81]. Toutefois, comme les décisions prises par ces organes subsidiaires de l'ONU en question n'ont aucune portée juridique contraignante, ces résolutions ont malheureusement fini dans les archives de la bibliothèque de l'ONU sans qu'une véritable coopération internationale sur ces sujets susmentionnés n'ait pris forme, et aucune coercition venant de ces organes subsidiaires ne peut être exercée à l'égard des États-membres de l'ONU pour que ceux-ci acquiescent l'importance des enjeux discutés dans les décisions prises lors de l'Assemblée générale. L'une des très rares instances d'organisations internationales dont les décisions ont un pouvoir juridique contraignant - et, donc, qui force les États-membres à appliquer ces décisions et à les intégrer à leur droit national interne pour qu'elles entrent en vigueur sur leur territoire - et qui pourrait potentiellement changer la donne en matière d'encadrement du cyberespace et du recours aux cyberarmes dans le cadre d'opérations stratégiques et militaires est le Conseil de Sécurité de l'Organisation des Nations unies. Le Conseil de Sécurité a entre

[81]Organisation des Nations unies. [s.d.] *La Première Commission adopte 15 projets de résolution et de décision dont deux projets concurrents sur la sécurisation du cyberespace*. Récupéré de : https://www.un.org/press/fr/2020/agdsi3659.doc.htm

autres le pouvoir d'appliquer des mesures coercitives pacifiques – sanctions - en cas de violation des principes fondamentaux de la Charte des Nations unies et du droit international humanitaire par ses États-membres, plus particulièrement lorsque ces violations mettent en péril la paix mondiale, dans le but de restaurer ou de maintenir cette dernière[82].

> Or, […] le Conseil ne dispose pas de ses propres instruments d'action. Il lui faut s'en remettre aux États membres pour faire appliquer, par leurs propres moyens, les mesures coercitives, et il reste tributaire de leur bon vouloir. L'aspect le plus visible est que le Conseil ne possède pas ses propres forces armées, et qu'il peut tout au plus autoriser des États agissant en son nom à employer la violence, voire à agir en leur nom propre dans le cadre de ses décisions[83].

Il est toutefois rarissime que le Conseil de Sécurité de l'ONU réussisse à adopter des nouvelles résolutions en matière de sécurité nationale, et cette parcimonie de décisions est notamment la résultante des multiples règles de cet organe en matière de processus décisionnel dont il sera question ultérieurement.

Le second enjeu juridique lié aux organisations internationales qui les empêche de mieux agir sur la scène internationale en matière d'amélioration du droit international humanitaire et de recours aux cyberarmes est, tel que mentionné dans le précédent paragraphe est la complexité de leur processus décisionnel. Ce processus est d'autant plus complexe lorsque les décisions d'une organisation internationale peuvent avoir un pouvoir juridique contraignant sur ses États-membres. Dans le cas de l'Organisation des Nations unies, chaque instance a un processus décisionnel qui lui est propre: par exemple, pour le Conseil de Sécurité, pour qu'une décision soit prise quant à une résolution ou un enjeu de sécurité internationale en particulier, celle-ci soit survivre à la fois à l'obtention d'une majorité absolue (9 des 15 membres du Conseil de Sécurité, où chaque État-membre a une voix au vote[84]) et au droit de veto des membres permanent du Conseil, qui peuvent appliquer ce droit à tout moment sauf sur les enjeux procéduraux du Conseil[85]. Ce droit de veto est souvent critiqué par la communauté internationale tant pour ses effets sur la représentativité de ses intérêts – puisqu'il est souvent utilisé pour mettre de l'avant les intérêts de l'État-membre qui l'exerce - que sur l'efficacité du processus décisionnel et sur le traitement d'enjeux de sécurité internationale, créant énormément de frustrations et de remises en question de la pertinence

---

[82] Sur, S. (2004). Le conseil de sécurité : blocage, renouveau et avenir. *Pouvoirs*, 109(2), p.61-74. https://doi.org/10.3917/pouv.109.0061

[83] Ibidem.

[84] Organisation des Nations unies. [s.d.] *Charte des Nations unies (Version intégrale)*. Récupéré de : https://www.un.org/fr/about-us/un-charter/full-text

[85] Ibidem.

du Conseil de Sécurité[86]. Les effets de l'échec des règles procédurales du Conseil de Sécurité sont de plus en plus dénoncés tant par des experts en matière de relations internationales que par des États-membres de l'ONU. Ceux-ci réclament depuis longtemps une réforme des procédures du Conseil de Sécurité en raison des bâtons dans les roues que causent le vote stratégique pour obtenir la majorité absolue - à travers lequel les États-membres auront tendance à prioriser leurs propres intérêts nationaux plutôt que les intérêts de la collectivité internationale - et le droit de veto des membres permanents du Conseil.

3.3. Cyber espionnage : stratégies et limites

Ce sont loin d'être toutes les cyber opérations ni tous les recours aux cyberarmes dans le cadre d'opérations stratégiques et militaires qui sont nécessairement des combats entre deux États ou qui sont nécessairement des attaques à effets destructeurs comme ce qui s'est passé avec l'Estonie et avec Stuxnet: dans plusieurs cas, certaines opérations étatiques menées dans le cyberespace sont beaucoup plus subtiles et cherchent plutôt à voler des informations plutôt qu'à en détruire. C'est entre autres le cas du cyber espionnage. La présente section de cette réflexion définira en quoi consiste le cyber espionnage, pourquoi et comment il est également utilisé par les États dans le cadre d'opérations stratégiques et militaires, et étudiera un cas typique de cyber espionnage pour appuyer le tout.

Selon l'Agence européenne pour la cybersécurité (ENISA), le cyber espionnage consiste en «l'utilisation des réseaux informatiques pour obtenir l'accès illicite à des informations confidentielles, généralement détenues par un gouvernement ou une autre organisation.[87]» Utilisant des techniques mentionnées dans le tout premier chapitre de cette réflexion, dont le phishing, le MITM et le recours à différents malwares/spywares (logiciels malveillants de surveillance) installés sur différents types d'appareils (ordinateurs, appareils mobiles, serveurs, etc.), le cyber espionnage est souvent utilisé par les États pour orchestrer des cyberattaques beaucoup plus discrètes dans le but d'acquérir des renseignements confidentiels sur un ou plusieurs autres États, que ce soit sur leur population, la santé de leur économie, leurs plans d'opérations militaires, des informations obtenues par leurs services de renseignements, et plus encore. Le tout se fait très souvent à distance sans que les cybers

[86]Sur, S. (2004). Le conseil de sécurité : blocage, renouveau et avenir. *Pouvoirs*, 109(2), p.61-74. https://doi.org/10.3917/pouv.109.0061

[87]ENISA. (2020) *Le cyber espionnage : Paysage des menaces de l'ENISA*. [Rapport annuel] DOI: 10.2824/552242

espions aient à se déplacer hors d'un centre de surveillance et de collecte de données. Dans un rapport annuel publié en 2020, l'ENISA discutait du cyber espionnage ainsi:

> En 2019, de nombreux rapports ont révélé que les organisations mondiales considéraient le cyber espionnage (ou espionnage parrainé par un État-nation) comme une menace croissante touchant les secteurs industriels ainsi que les infrastructures critiques et stratégiques du monde entier, notamment les ministères, les compagnies ferroviaires, les opérateurs de télécommunications, les sociétés d'approvisionnement en énergie, les hôpitaux et les banques. Le cyber espionnage se concentre sur des enjeux géopolitiques et sur le vol de secrets d'État, de secrets d'affaires, de droits de propriété intellectuelle et de renseignements exclusifs dans des domaines stratégiques. Il mobilise également des acteurs de l'économie, de l'industrie et des services de renseignement extérieur, ainsi que des acteurs travaillant en leur nom. Dans un récent rapport, les analystes du renseignement sur la menace n'ont pas été étonnés d'apprendre que 71 % des organisations traitaient le cyber espionnage, ainsi que d'autres menaces, comme une « boîte noire » et qu'elles en apprenaient encore tous les jours sur le sujet[88].

Les services de renseignements de plusieurs États ont de plus en plus recours au cyber espionnage comme stratégie pour collecter des informations et pour surveiller des potentielles menaces pour les mêmes raisons que les États choisissent d'avoir recours à des cyber unités de combat. (Voir section 1.2 du chapitre 1 de cette réflexion) Ces secrets d'État volés plus rapidement, plus efficacement et à moindre coûts leur donnent un avantage considérable sur la scène internationale sur les plans économique, politique, social et militaire. Ils sont souvent utilisés dans le cadre de chantage (*blackmail*) et de menaces à l'égard d'un autre État - surtout si les informations volées mettent l'État en question dans une position compromettante - , mais également dans le cadre de négociations d'accords et de traités.

En droit international, la question du cyber espionnage - surtout en temps de paix - est largement débattue et controversée par les juristes, car elle tombe dans l'angle mort de tous les cadres juridiques existants : en effet, à l'heure actuelle, aucune convention internationale ni traité n'encadre ni ne sanctionne le cyber espionnage. D'une part, certains juristes ne veulent pas faire de distinction entre espionnage et cyber espionnage - et soutiennent donc que les mêmes règles actuelles en matière d'espionnage s'appliquent de la même façon tant dans le monde réel que dans le monde virtuel -, et d'une autre, d'autres juristes soutiennent qu'en raison des techniques différentes utilisées dans le cyber espionnage versus l'espionnage «traditionnel», il est impératif d'avoir un cadre juridique différent avec des sanctions

[88]ENISA. (2020) *Le cyber espionnage : Paysage des menaces de l'ENISA*. [Rapport annuel] DOI: 10.2824/552242

différentes. Présentement, en temps de guerre, l'un des protocoles des Conventions de Genève prévoit les règles suivantes en matière d'espionnage :

> Aux termes de l'article 24 du Règlement de La Haye, l'emploi des moyens nécessaires pour se procurer des renseignements sur l'ennemi et sur le terrain est considéré comme licite. Ces renseignements peuvent bien souvent être obtenus par des moyens, sinon toujours décelés, du moins ouvertement utilisés à cette fin: écoutes, photographies aériennes, explorations au sol, etc. [...] C'est alors qu'intervient l'espionnage, c'est-à-dire le recours à l'agent secret, que le droit international applicable en cas de conflit armé, écrit ou coutumier, n'interdit pas, tout en laissant la liberté aux Etats de punir les espions qui agissent à leur détriment. En temps de conflit armé, l'espion n'engage donc pas la responsabilité internationale de l'Etat qui l'envoie. L'espionnage proprement dit, qui peut être indifféremment le fait d'une personne civile ou d'un membre des forces armées agissant en secret, se distingue traditionnellement de ce qu'on a appelé autrefois la « trahison de guerre », qui consiste notamment, mais pas exclusivement, pour une personne civile habitant en territoire occupé, à donner des renseignements à l'ennemi de l'occupant. Le « traître de guerre » viole la loi de l'occupant[89].

Comme le cyber espionnage ne se fait pas nécessairement en temps de guerre et que les espions n'ont pas nécessairement besoin d'interagir avec la population locale de l'État espionné, il n'est pas - techniquement - légal d'avoir recours aux cyberarmes pour mener des opérations de cyber espionnage, mais encore une fois, celles-ci ne sont - techniquement - pas condamnées non plus. À l'heure où les technologies de l'information et des communications sont au cœur de notre quotidien - dont des cyber opérations et de la vie politique - , ce flou et cette faille dans le cadre juridique entourant le cyberespace et l'espionnage est une autre preuve des limites de celui-ci.

Le cyberespionnage peut prendre une pléthore de formes différentes, et avec l'embarras du choix de techniques et de technologies à leur disposition pour mener leurs opérations à termes, les espions ne manquent pas d'imagination pour arriver à leurs fins. Il existe des centaines de cas différents de cyberespionnage survenus au cours des dix dernières années qui n'ont pas été réclamés par leurs auteurs, que ce soit des États ou des groupes non-étatiques d'espions et de *hackers*. L'un des cas des dix dernières années touchant directement le Canada est la mission de cyber espionnage perpétrée par la Chine en 2014.

---

[89]Comité international de la Croix-Rouge. [s.d.] *Traités, États parties et Commentaires - Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), 8 juin 1977*. Récupéré de : https://ihl-databases.icrc.org/dih-traites/COM/470-750056?OpenDocument

> Le 23 juillet 2014, le gouvernement Harper affirmait, par voie de communiqué, que le Conseil national de recherches du Canada (CNRC) avait été victime d'une opération de cyber espionnage d'envergure commanditée par l'État chinois. Ironie du sort ? Cette cyber opération survenait au moment où le CNRC travaillait à l'élaboration d'un système de communication « inviolable », capable justement de prévenir de telles activités clandestines. D'après le bilan officiel de l'événement, le gouvernement canadien attribue la faute à un acteur hostile parrainé par l'État chinois, lequel a ouvert une brèche dans les réseaux du CNRC par l'entremise d'un logiciel malveillant contenu dans un courriel. Les pirates auraient vraisemblablement pu se procurer non seulement des renseignements sensibles sur des projets et programmes de recherche en cours, mais aussi des données personnelles d'employées et d'employés du CNRC. L'intrusion, une fois détectée, a aussitôt conduit à la fermeture du système informatique du Conseil. Le prix à payer ? Une faramineuse facture de 32,5 millions de dollars, acquittée par le gouvernement fédéral afin de rétablir les réseaux de l'institution. La Chine, de son côté, a nié les allégations à son égard, affirmant que le Canada l'accusait sans la moindre preuve[90].

Ce cas de cyber espionnage État à État en temps de paix - les relations étaient plutôt tendues entre la Chine et le Canada à l'époque, mais aucun état de guerre n'a été déclaré - est une preuve des dégâts non-négligeables pour la population canadienne que peuvent causer le recours à des opérations cybernétiques, aux cyberarmes et le manque d'encadrement juridique du cyberespace.

3.4. Recommandations juridiques d'améliorations en matière de traitement d'enjeux de cybersécurité

Maintenant que les enjeux juridiques autour du recours aux cyberarmes aient été étudiés - notamment en analysant le cadre juridique actuel autour de cette question, ses failles et les limites juridiques aux façons dont les organisations internationales peuvent contribuer à son amélioration -, des recommandations en matière de traitement et de résolution de ces enjeux sont de mise. À la lueur de la littérature existante, la présente partie de cette réflexion portera sur deux recommandations qu'il serait possible de faire aux dirigeants politiques de la scène internationale pour éventuellement résorber lesdits enjeux juridiques dont il a été question plus tôt au cours de cette réflexion.

---

[90]Gagnon, F. et al. (2021, mars) *Cyberincidents géopolitiques au Canada : Un état des lieux proposé par l'Observatoire des conflits multidimensionnels*. [Rapport] Chaire Raoul-Dandurand. https://dandurand.uqam.ca/wp-content/uploads/2021/03/Rapport-cyberincidents_OCM_2021.pdf

La toute première recommandation à faire pour améliorer le traitement d'enjeux juridiques liés à l'usage de cyberarmes est, sans surprise, de revoir le cadre juridique en la matière. Tel que mentionné plus tôt, la Convention de Budapest de 2004 du Conseil de l'Europe et les événements cybernétiques en Estonie ont permis à plusieurs États à travers le monde de se doter d'un cadre juridique national de base en matière de cybersécurité et de recours aux cyberarmes. Des suites de ces événements et après que de nombreuses organisations internationales aient sonné l'alarme sur la dangerosité quant au manque d'encadrement juridique à jour des cyberarmes, quelques initiatives intergouvernementales et quelques efforts de coopération internationale à ce sujet, comme des sommets et des conférences, ont pris forme au cours des dernières années pour discuter de la possibilité de créer un nouveau cadre juridique international à part entière qui permettrait de prévenir les actes de violences cybernétiques - peu importe leur forme - et de les sanctionner en cas d'infraction. Toutefois, comme les acteurs étatiques, qui sont les seuls à véritablement avoir le pouvoir de créer et d'améliorer un cadre juridique adéquat pour n'importe quel enjeu touchant la communauté internationale, ne sont jamais arrivés à trouver un terrain d'entente ni sur le contenu exact de ce nouveau cadre juridique ni sur sa forme, ces initiatives n'ont malheureusement jamais abouti concrètement sur quoi que ce soit. Tel est le cas, par exemple, de la proposition de traité international en matière de cybersécurité et de cybercriminalité transnationales déposée par la Russie en 2019 - appuyée par une vingtaine d'États asiatiques et moyen-orientaux, dont le Cambodge et la Chine - qui prévoit de resserrer les termes et les sanctions prévues par l'actuelle Convention de Budapest du Conseil de l'Europe, et ce, bien que la Russie n'en soit présentement pas signataire. Bien qu'une initiative de la sorte soit réclamée depuis plusieurs années par les organisations internationales et plusieurs États sur la scène internationale, des organisations internationales non-gouvernementales comme Human Rights Watch expriment dans les médias de masse leurs inquiétudes et leurs réserves quant à ce projet de traité, puisque le projet présenté par la Russie implique notamment des restrictions en termes de droit d'expressions, d'association, de respect de la vie privée et de d'application du droit international[91]. Bien que les différents gouvernements de ce monde bénéficieraient largement d'un nouveau cadre juridique international en matière de cybersécurité, de recours aux cyberarmes et de cybercriminalité transnationale, il est primordial que ce nouveau cadre juridique revu et corrigé priorise la sécurité et le bien-être de

[91]Brown, D. (2021, 13 août) Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights. In *Human Rights Watch*. Récupéré de : https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights#

chaque être humain de la communauté internationale plutôt que les intérêts stratégiques de l'agenda des dirigeants d'États.

Ensuite, la seconde recommandation à faire pour améliorer le traitement d'enjeux juridiques liés à l'usage de cyberarmes est de revoir les règles de fonctionnement de certaines organisations internationales, à commencer par les doter du pouvoir de se saisir de questions de cybersécurité, incluant les opérations militaires cybernétiques et les moyens, dont les outils, qui sont utilisés dans le cadre de celles-ci. En effet, dans les règles de fonctionnement des organisations internationales, et plus particulièrement, du Conseil de Sécurité, il n'y a pas que la question des règles de vote et du recours au droit de veto qui posent problèmes : présentement, comme le Conseil de Sécurité a énormément de dossiers et d'enjeux à gérer simultanément, celui-ci délègue l'étude de certains enjeux à d'autres organisations internationales onusiennes qu'il juge plus compétentes en la matière. Par exemple, dans le cas des questions touchant le cyberespace, l'UNODC[92] (L'Office des Nations unies contre les drogues et le crime) et l'UNIDIR (L'Institut des Nations unies pour la recherche sur le désarmement) sont présentement les deux organisations internationales onusiennes en charge de ce type de dossiers et d'enjeux[93]. Le problème ici est le fait que, tel que discuté plus tôt dans cette réflexion, ces deux organisations internationales susmentionnées n'ont pas le pouvoir de produire des documents qui sont juridiquement contraignants[94]. L'ONU a donc deux options devant elle : la première serait qu'elle décide de rapatrier toutes les questions touchant au cyberespace - et donc, de surcroît, au recours aux cyberarmes - à son Conseil de Sécurité pour que ses membres puissent légiférer sur la question, et ce, au risque que chaque proposition de projets de traité tombe à l'eau à cause de l'utilisation abusive du droit de veto par ses membres permanents. La deuxième option qui lui est présentée serait qu'elle octroie à ses autres organisations internationales compétentes, comme l'UNIDIR et l'UNODC, - dont les membres n'ont pas de droit de veto - le pouvoir de se saisir juridiquement de ce type d'enjeux et de créer d'elles-mêmes un cadre juridique adéquat en matière d'enjeux cybernétiques. Cette deuxième option permettrait d'accélérer le processus d'amélioration du droit international en matière de sécurité internationale et de recours aux cyberarmes sans trop empiéter sur la souveraineté des États.

---

[92] UNODC. [s.d.] *The United Nations Office on Drugs and Crime*. Récupéré de : https://www.unodc.org/
[93] UNIDIR. [s.d.] *The United Nations Institute for Disarmament research*. Récupéré de : https://unidir.org/
[94]Organisation des Nations unies. [s.d.] *Charte des Nations unies (Version intégrale)*. Récupéré de : https://www.un.org/fr/about-us/un-charter/full-text

Conclusion

La présente réflexion avait pour but d'étudier comment, au cours des dernières décennies, le recours aux cyberarmes et aux opérations cybernétiques offensives et défensives par les corps militaires et par les services de renseignements de différents États ont-ils contribué à créer de nouveaux enjeux de sécurité nationale et internationale. Somme toute, il a été possible de confirmer que de multiples enjeux politiques et juridiques liés au recours à du matériel informatique et aux nouvelles technologies dans le cadre d'opérations stratégiques et militaires se sont créés au fil des ans, et que d'autres risquent d'apparaître également avec l'avènement d'autres technologies plus sophistiquées. Il a notamment été question que la communauté politique et juridique leur porte une attention plus particulière qu'à l'heure actuelle à l'identification et au contrôle des cyberarmes, à l'adoption d'une définition politico-juridique claire et reconnue par la communauté internationale d'une cyberattaque, d'une cyberarme et du cyber espionnage, à l'adoption d'un cadre juridique adéquat régulant les questions cybernétiques ainsi qu'aux conséquences sociales, économiques et politiques tant pour les États que pour la population civile de l'utilisation de cyberarmes.

Après un chapitre faisant l'état des lieux sur les questions cybernétiques et sur les concepts liés au cyberespace, il a été question au cours de cette réflexion des différents enjeux politiques liés au cyberespace, comme les conséquences réelles et potentielles du recours aux cyberarmes pour la population civile et ses institutions ainsi que les changements dans les rapports de force observables sur la scène internationale découlant de ce recours aux cyberarmes. Étant donné les contraintes matérielles de cette réflexion, afin de comprendre l'ampleur de ce phénomène croissant et afin de discuter des principaux acteurs et événements qui sont liés au recours aux cyber opérations stratégiques et militaires défensives et offensives, il a fallu se limiter à l'étude de 4 grands acteurs étatiques du cyberespace - soit les États-Unis, le Canada, la Chine et la Russie - et de 2 cas de figure de cyberattaques État à État qui ont marqué l'imaginaire collectif - soit les cas de Stuxnet et de l'Estonie. L'étude de ces enjeux et de ces acteurs politiques a aussi permis de réfléchir d'émettre des recommandations pour pouvoir améliorer le traitement de ces enjeux. La première recommandation émise était de mieux éduquer et d'éduquer davantage la population - et surtout, les dirigeants politiques - sur les questions de cybersécurité pour qu'ils comprennent mieux la portée de leurs décisions et de leurs actions visant le cyberespace. La deuxième recommandation en la matière, visant encore une fois les dirigeants politiques, était d'investir davantage dans la recherche et le développement de cyber unités de combat, étant donné que de plus en plus d'opérations

militaires se tiendront dans le cyberespace plutôt que sur le terrain « réel ». Afin de compléter cette réflexion, il aurait également été intéressant d'étudier davantage d'acteurs étatiques du cyberespace - comme par exemple les cas de la France, la Corée du Nord, l'Inde, le Pakistan et l'Australie -, d'étudier la contribution d'acteurs non-étatiques aux cyber opérations offensives (ex.: mercenaires, hackers, terroristes, etc.) et d'étudier plus de cas de figure de cyberattaques État à État ou acteur non-étatique à État, comme les multiples cas de cyberattaques russes et chinoises - non réclamées officiellement par leurs gouvernements respectifs, bien sûr - qui ont été perpétrées à l'égard de différentes agences ministérielles américaines et canadiennes au cours des cinq dernières années.

Par la suite, après avoir discuté des différents enjeux politiques liés au cyberespace, il a été question au cours de cette réflexion des différents enjeux juridiques de ce même sujet. Il a été question à plusieurs reprises des multiples failles dans le cadre juridique actuel en matière d'opérations cybernétiques et de recours aux cyberarmes résultant notamment de l'obsolescence de celui-ci et du manque de coopération intergouvernementale pour le mettre à jour et y intégrer des concepts et des pratiques qui n'existaient pas au moment de la création dudit cadre juridique en question. Il a également été question de différents enjeux en lien avec la place des organisations internationales - surtout celles appartenant au système onusien - dans la mise en place et dans le renforcement du cadre juridique international autour des questions cybernétiques, et plus précisément, des freins qui les empêchent de prendre part davantage à la conception et à la mise à jour dudit cadre juridique susmentionné. Les principaux freins juridiques étudiés ont été la personnalité juridique de ces organisations internationales, leurs règles de fonctionnement prévues par leur charte et la délégation de dossiers d'organes subsidiaires compétents en cybersécurité internationale et en cyber opérations militaires - c'est-à-dire le Conseil de Sécurité - à des organisations internationales spécialisées sur ces enjeux, mais qui ne détiennent pas le pouvoir d'agir sur ceux-ci - comme l'UNODC et l'UNIDIR. Cette réflexion a aussi permis de mettre en lumière des débats autour de la légalité du cyber espionnage et des limites de celui-ci. Tout comme dans le chapitre sur les enjeux politiques liés au cyberespace, à la lumière de la littérature mobilisée pour analyser les événements et les concepts étudiés au cours de cette réflexion, deux recommandations de nature juridique ont été émises. La première recommandation émise - et la plus évidente - est de revoir le contenu du cadre juridique international en la matière pour que les autorités compétentes puissent l'améliorer, le mettre à jour et le rendre adéquat tant à la situation actuelle qu'aux éventualités à prévoir sur le long terme. La seconde recommandation faite a

été de revoir les règles de fonctionnement des organisations internationales onusiennes, surtout en matière de participation à la création du cadre juridique susmentionné et de la possibilité de légiférer sur ce sujet tout en respectant la souveraineté de leurs États-membres : l'ONU doit revoir quelles organisations et quels organes peuvent prendre des décisions à portée juridique contraignante et lesquels peuvent uniquement conseiller et éduquer leurs États-membres sur différents enjeux. Il aurait été intéressant, au cours de cette réflexion, d'aborder les différentes conséquences réelles découlant des règles de fonctionnement du système onusien en analysant des cas de figure concrets de décisions prises par le Conseil de Sécurité de l'ONU en matière de cybersécurité internationale et de recours aux cyberarmes afin de voir dans quelles circonstances le droit de veto est utilisé ainsi que les raisons derrières le refus de prendre des décisions contraignantes pour les États-membres à propos du cyberespace.

Étant donné les contraintes matérielles de cette réflexion, et comme les enjeux liés au cyberespace se font de plus en plus nombreux, il serait important et intéressant d'exploiter et d'explorer, dans une prochaine réflexion semblable, les enjeux politiques et juridiques liés au cyberterrorisme, qui est également une forme de cyberattaque dont le nombre d'opérations offensives a cru d'années en années au cours de la dernière décennie, et de son encadrement dans le droit international pour les mêmes raisons que celles mentionnées tout au long de la présente réflexion. Il serait intéressant d'étudier ce sujet en abordant les différences entre le « traditionnel/conventionnel » et le cyberterrorisme, pourquoi ce phénomène prend de l'ampleur, quels sont les acteurs impliqués dans la production du cyberterrorisme ainsi que dans la lutte contre celui-ci ainsi que les initiatives politico-juridiques existantes qui ont été mises sur pied par la communauté internationale pour étudier ce phénomène et le freiner. Dans un rapport d'une quarantaine de pages publié en 2014, l'UNODC sonnait l'alarme de cette façon quant au cyberterrorisme :

> La menace fondamentale constituée par la propagande terroriste concerne la manière dont elle est utilisée et l'intention dans laquelle elle est diffusée. La propagande diffusée sur Internet vise tout un éventail d'objectifs et de publics. Elle peut être adaptée, entre autres, aux sympathisants ou opposants potentiels ou effectifs d'une organisation ou d'un courant extrémiste, aux victimes directes ou indirectes d'actes de terrorisme, à la communauté internationale ou à une partie de celle-ci. [...] Parmi les autres objectifs de la propagande terroriste, on peut citer le recours à la manipulation psychologique pour fragiliser la croyance d'une personne dans certaines valeurs sociales collectives, ou pour accroître le sentiment d'anxiété, de peur

> ou de panique au sein d'une population ou d'une partie de celle-ci. La diffusion de désinformation, de rumeurs, de menaces de violence ou d'images d'actes de violence provocants permet d'atteindre ces objectifs. Le public visé comprend les spectateurs directs de ces contenus, ainsi que les personnes touchées par la publicité potentielle en découlant. En ce qui concerne la communauté internationale au sens plus large, l'objectif est souvent de véhiculer un désir d'atteindre des objectifs politiques nobles[95].

Il serait également intéressant de s'attarder au rôle des acteurs étatiques et non-étatiques dans la cybercriminalité transnationale, à savoir quelles sont leurs motivations qui les poussent à avoir recours au cyberespace pour commettre leurs crimes, comment la cybercriminalité a évolué au cours des vingt dernières années, comment ce recours au cyberespace a changé leurs façons de commettre certains crimes (comparativement à une méthode plus tangible et traditionnelle de faire les choses), quelles sont les initiatives prises pour prévenir et contrer ce phénomène en vogue, et plus encore. Étant donné le contexte sanitaire des deux dernières années, il serait intéressant également de voir comment la pandémie de COVID-19 a contribué à ce recours au cyberespace tant dans le cadre d'opérations stratégiques et militaires, mais également dans le cadre d'opérations criminelles et terroristes tant à l'échelle nationale qu'internationale.

[95]UNODC. (2014, mars) *Utilisation d'Internet à des fins terroristes*. [Rapport] https://www.unodc.org/documents/terrorism/Publications/The_Use_of_Internet_for_Terrorist_Purposes/Use_of_the_Internet_for_Terrorist_Purposes_French.pdf

BIBLIOGRAPHIE

- Adonis, A. (2020, 14 mars) International Law on Cyber Security in the Age of Digital Sovereignty. *E-International Relations*. Récupéré de : https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/
- Affaires mondiales Canada. [s.d.] *Le Canada exprime son inquiétude face aux activités malveillantes des services de renseignements militaires russes*. Récupéré de : https://www.canada.ca/fr/affaires-mondiales/nouvelles/2020/10/le-canada-exprime-son-inquietude-face-aux-activites-malveillantes-des-services-de-renseignements-militaires-russes.html
- Akbariavaz, K. et Tehrani, P.M. (2020). *Cyberattacks and the Prohibition of the Use of Force under Humanitarian Law with Reference to the Tallin Manual: Cyberattacks and Humanitarian Law*, Bolton, Eliva Press.
- Artese, E. et Vitkov, V. (2015, novembre) Cyberwarfare and Collateral Damages. In *Globalex*. Récupéré de: https://www.nyulawglobal.org/globalex/Cyberwarfare_Collateral_Damages.html
- Azoulay, A. (2019) Towards an ethics of artificial intelligence. *UN Chronicle*, 55 (4), 24-25.
- Barnard-Wills, D., & Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture*, 15(2), 110–123. DOI: https://doi.org/10.1177/1206331211430016
- Bannelier, K. et Christakis, T. (2017). Cyberdéfense active par des entreprises privées ? Le hack-back entre l'hostilité de la Revue Stratégique de cyberdéfense de la France et le projet de loi ACDC aux États-Unis. *Stratégique*, 4 (117), 99-118. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0099
- Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, 44(2), 147–164. DOI: https://doi.org/10.1177/0967010613478323
- Britannica, T. Editors of Encyclopaedia (2021, 2 août). Enigma. In *Encyclopedia Britannica*. Récupéré de : https://www.britannica.com/topic/Enigma-German-code-device
- Brown, D. (2021, 13 août) Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights. *Human Rights Watch*. Récupéré de : https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights#
- Boily, D. (2021, 8 décembre) Vol massif de données : l'ex-employé aurait tout avoué à la direction de Desjardins. In *Radio-Canada Informations*. Récupéré de : https://ici.radio-canada.ca/nouvelle/1845776/vol-massif-donnees-ex-employe-confession-direction-desjardins
- Canadian Association of Defence and Security Industries. (2019) [s.d.] *2019 Annual Report - From Bullets to Bytes : Industry's role in preparing Canada for the future of Cyber Defence*. Récupéré de : https://www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-24.pdf
- Cattaruzza, A. (2017). Penser les limites de la numérisation du champ de bataille. *Stratégique*, (4) 117, 41-58. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0041

- Center for Strategic and International Studies. [s.d.] *Strategic Technologies Program*. Récupéré de : https://www.csis.org/programs/strategic-technologies-program
- Chiva, E. (2019). L'intelligence artificielle : un moteur de l'innovation de défense française. *Revue Défense Nationale*, 5 (820), 33-37. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/rdna.820.0033
- Chong, A. (2014). Information Warfare?: The Case for an Asian Perspective on Information Operations. *Armed Forces & Society*, 40(4), 599–624. DOI: https://doi.org/10.1177/0095327X13483444
- CISA. [s.d.] *Cybersecurity*. Récupéré de : https://www.cisa.gov/cybersecurity
- Colombani, J. (2016). *Cyberespace et Terrorisme*, Québec, Les Presses de l'Université Laval.
- Comité international de la Croix-Rouge. [s.d.] *Conduite des hostilités et droit international humanitaire*. Récupéré de : https://www.icrc.org/fr/document/conduite-des-hostilites
- Comité international de la Croix-Rouge. (2009) *Glossaire : Termes utilisés dans le programme EDH*. [Glossaire] https://www.icrc.org/en/doc/what-we-do/building-respect-ihl/education-outreach/ehl/ehl-other-language-versions/ehl-french-glossary.pdf
- Comité international de la Croix-Rouge. [s.d.] *New Technologies and IHL*. Récupéré de : https://www.icrc.org/en/war-and-law/weapons/ihl-and-new-technologies
- Comité international de la Croix-Rouge. [s.d.] *Traités, États parties et Commentaires - Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), 8 juin 1977*. Récupéré de : https://ihl-databases.icrc.org/dih-traites/COM/470-750056?OpenDocument
- Comité international de la Croix-Rouge. (2021, 25 février) *Le droit international humanitaire peut-il limiter la cyberguerre?* Récupéré de : https://www.icrc.org/fr/document/Le-droit-international-humanitaire-peut-il%20limiter-la-cyberguerre%3F
- CRPC. [s.d.] *Lutter contre les cybermenaces pesant sur les institutions financières au Canada: étude qualitative d'une approche de partenariat public-privé pour protéger des infrastructures critiques*. Récupéré de : https://www.prevention-cybercrime.ca/lutte-contre-les-cybermenaces
- *Convention sur la cybercriminalité*, 2001, STE 185 –23.XI.2001 (entrée en vigueur le 1er juillet 2004) [Conseil de l'Europe]
- Council of Europe. [s.d.] *Chart of signatures and ratifications of Treaty 185*. Récupéré de : https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185
- Coustillière, A. (2016). Le combat numérique au cœur des opérations : quels enjeux pour le monde maritime ? *Revue Défense Nationale*, 789, 44-48. https://doi.org/10.3917/rdna.789.0044
- Danet, D. (2017). Collapsologie numérique. *Stratégique*, 4 (117), 213-230. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0213
- de Lespinois, J. (2017). Guerre et paix dans le cyberespace. *Stratégique*, 4 (117), 155-168. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0155
- Döge, J. (2010). Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime. *Archiv Des Völkerrechts*, 48 (4), 486-501. Récupéré de : http://www.jstor.org/stable/25782613

- Douzet, F., Limonier, K., Robine, J., Salamatian, K., Géraud, R. & Campigotto, R. (2017). Les nouveaux territoires stratégiques du cyberespace : le cas de la Russie. *Stratégique*, 4 (117), 169-186. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0169
- Domingo, F. C. (2016). China's Engagement in Cyberspace. *Journal of Asian Security and International Affairs*, 3(2), 245–259. DOI: https://doi.org/10.1177/2347797016645456
- Durham, H. (2020, 26 mars) Les cyberopérations en période de conflit armé : 7 questions juridiques et politiques essentielles. In *CICR*. Récupéré de : https://blogs.icrc.org/law-and-policy/fr/2020/03/26/cyber-armed-conflict-7-law-policy-questions/
- Eakin, H. (2017). Les Suédois, rois de la cyberguerre. *Books*, 7-8 (84), 22-27. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/books.084.0022
- ENISA. (2020) *Le cyberespionnage : Paysage des menaces de l'ENISA*. [Rapport annuel] DOI: 10.2824/552242
- Etcheverry, P. (2018). *Cyber et Drones*, Paris, Economica.
- Exportation et Développement Canada. (2018, 24 janvier) La gestion des cyber risques : un sujet incontournable en 2018. In *ExportActions*. Récupéré de : https://www.edc.ca/fr/article/2018-cyber-risk-management.html
- Gagnon, F. et al. (2021, mars) *Cyberincidents géopolitiques au Canada : Un état des lieux proposé par l'Observatoire des conflits multidimensionnels*. [Rapport] Chaire Raoul-Dandurand. https://dandurand.uqam.ca/wp-content/uploads/2021/03/Rapport-cyberincidents_OCM_2021.pdf
- Gendarmerie royale du Canada. (2014) *Cybercriminalité : survol des incidents et des enjeux au Canada.* [Rapport] https://www.rcmp-grc.gc.ca/fr/cybercriminalite-survol-des-incidents-et-des-enjeux-au-canada >
- Gouvernement du Canada. [s.d.] *Cyber Operator*. Récupéré de : https://forces.ca/en/career/cyber-operator/
- Gouvernement du Canada. [s.d.] *Infographie pour Cyberforces et systèmes de communication et d'information (SCI) interarmées prêts au combat*. Récupéré de : https://www.tbs-sct.gc.ca/ems-sgd/edb-bdd/index-fra.html#orgs/program/ND-BUO06/infograph/financial
- Gouvernement du Canada. [s.d.] *Infographie pour Cyberopérations*. Récupéré de : https://www.tbs-sct.gc.ca/ems-sgd/edb-bdd/index-fra.html#orgs/program/ND-BUN05/infograph/financial
- Gouvernement du Canada. [s.d.] *Infographie pour Défense nationale*. Récupéré de : https://www.tbs-sct.gc.ca/ems-sgd/edb-bdd/index-fra.html#orgs/dept/133/infograph/financial
- Gouvernement du Canada. [s.d.] *Politique internationale en matière de cyberespace*. Récupéré de : https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyber_policy-politique_cyberspace.aspx?lang=fra
- Gouvernement du Canada. [s.d.] *Un gouvernement juste et responsable*. Récupéré de : https://www.budget.gc.ca/2021/report-rapport/p4-fr.html

- Govella, K. (2021). China's challenge to the global commons: compliance, contestation, and subversion in the maritime and cyber domains. *International Relations*. DOI: https://doi.org/10.1177/00471178211036228
- Haddad, S. (2017). Une grammaire de la cybersécurité française ou la construction d'une stratégie nationale de cyberdéfense (2008-2017). *Stratégique*, 4 (117), 119-135. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0119
- Hansel, M., & Ruhnke, S. (2017). A revolution of democratic warfare? Assessing regime type and capability-based explanations of military transformation processes. *International Journal*, 72(3), 356–379. DOI: https://doi.org/10.1177/0020702017724806
- Hearn, K. (2017). Book Review: Cyber Policy in China. *Media International Australia*, 163(1), 176–176. DOI: https://doi.org/10.1177/1329878X17710385
- Hérisson, A. (2017). Le cyberespace, cet espace de confrontation à part entière. *Stratégique*, 4 (117), 231-246. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0231
- Hoorickx, E. (2017). Une cyberstratégie euro-atlantique en matière de défense : mythe ou réalité ?. *Stratégique*, 4 (117), 187-202. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0187
- Hugues, R. (2009) Towards a Global Regime for Cyber Warfare. Dans *The Virtual Battlefield : Perspective on Cyber Warfare*. Amsterdam, IOS Press Books (3e volume, p.106-117) Récupéré de : https://ccdcoe.org/uploads/2018/10/07_HUGHES-Cyber-Regime.pdf
- International group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence et Schmitt, M. (dir.). (2017) *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations* (2e ed.). Cambridge, Cambridge University Press.
- Institute for Strategic Studies. [s.d.] *China's new Five-Year Plan and 2021 budget: what do they mean for defence?*. Récupéré de : https://www.iiss.org/blogs/analysis/2021/03/chinas-new-five-year-plan-and-2021-budget
- Imperial War Museum. (2021) [s.d.] *How Alan Turing Cracked the Enigma Code?* Récupéré de : https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code
- Jomni, A. (2018). Le Darknet est-il une zone de non droit ?. *Sécurité globale*, 3 (15), 17-23. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/secug.183.0017
- Kaushik, K. (2021, 27 avril) India third highest military spender in 2020, states data published by Stockholm International Peace Research Institute. In *Indian Express*. Récupéré de : https://indianexpress.com/article/india/india-third-highest-military-spender-in-2020-7290118/
- Kello, L. (2014). Les cyberarmes : dilemmes et futurs possibles. *Politique étrangère*, numéro 4 , 139-150. DOI : https://doi.org/10.3917/pe.144.0139
- Kempf, O. (2017). Des différences entre la cybersécurité et la transformation digitale. *Stratégique*, (4) 117, 59-64. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0059
- Le Monde avec AFP. (2021, 8 septembre) Cybersécurité : la défense française veut renforcer ses troupes de cybercombattants. In *Le Monde*. Récupéré de: https://www.lemonde.fr/pixels/article/2021/09/08/cybersecurite-la-defense-francaise-etoffe-ses-troupes-de-cybercombattants_6093949_4408996.html

- Maness, R. C., & Valeriano, B. (2016). The Impact of Cyber Conflict on International Interactions. *Armed Forces & Society*, 42(2), 301–323. DOI: https://doi.org/10.1177/0095327X15572997
- Marks, J., et Schaffer, A. (2021, 21 juin) The Cybersecurity 202: Legal scholars are working on new rules for international hacking conflicts. *The Washington Post*. Récupéré de : https://www.washingtonpost.com/politics/2021/06/21/cybersecurity-202-legal-scholars-are-working-new-rules-international-hacking-conflicts/
- Ministère de la Défense du Japon. (2021) *Defense Programs and Budget of Japan - Overview of FY2021 Budget* [Rapport budgétaire annuel] https://www.mod.go.jp/en/d_act/d_budget/pdf/210331a.pdf
- Ministère des Armées. [s.d.] *La cyberdéfense*. Récupéré de : https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/mission
- NATO Cooperative Cyber Defence Centre of Excellence. [s.d.] *A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons*. Récupéré de : https://ccdcoe.org/uploads/2018/10/8_d1r2s6_raymond.pdf
- NATO Strategic Communications Center of Excellence. [s.d.] *Hybrid Threats: 2007 cyber attacks on Estonia*. Récupéré de : https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86
- NATO Strategic Communications Centre of Excellence. (2021) [s.d.] *Russia's Strategy in Cyberspace*. Récupéré de : https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf
- Nocetti, J. (2014). Puissances émergentes et internet : vers une « troisième voie » ?. In *Politique étrangère,* numéro 4 , 43-55. DOI: https://doi.org/10.3917/pe.144.0043
- Office québécois de la langue française. [s.d.] *Cyberattaque*. Récupéré de : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8351162
- Ohlin, J. et al. (2015) *Cyberwar : law and ethics for virtual conflicts*. Oxford, Oxford University Press. DOI:10.1093/acprof:oso/9780198717492.003.0004
- Organisation des Nations unies. [s.d.] *Charte des Nations unies (Version intégrale)*. Récupéré de : https://www.un.org/fr/about-us/un-charter/full-text
- Organisation des Nations unies. [s.d.] *La Première Commission adopte 15 projets de résolution et de décision dont deux projets concurrents sur la sécurisation du cyberespace*. Récupéré de : https://www.un.org/press/fr/2020/agdsi3659.doc.htm
- Organisation des Nations unies. (2019) *The Age of Digital Interdependence*. Récupéré de : https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf
- RAND Corporation. [s.d.] *Cyber Warfare*. Récupéré de : https://www.rand.org/topics/cyber-warfare.html
- Raufer, X. (2018). Une excursion (guidée) au Far-West numérique. *Sécurité globale*, 3 (15), 49-69.DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/secug.183.0049
- Rolland, E. (2017). Quel modèle d'armée numérique pour demain ?. *Stratégique*, 4 (117), 203-212. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0203
- Romanosky, S., et Goldman, Z. (2017, 6 octobre) Understanding Cyber Collateral Dammage. In *Journal of National Security Law and Policy*, 9 (2). https://jnslp.com/2017/10/06/understanding-cyber-collateral-damage/
- Rompré, A. (2021) *Digitalisation des forces armées: enjeux de sécurité nationale et internationale liés à l'utilisation de matériel informatique dans le cadre d'opérations*

stratégiques et militaires. [Projet de travail dirigé, document non publié]. Université du Québec à Montréal.

- Rowe, C., Seif Zadeh, H., Garanovich, I. L., Jiang, L., Bilusich, D., Nunes-Vaz, R., et Ween, A. (2019). Prioritizing investment in military cyber capability using risk analysis. *The Journal of Defense Modeling and Simulation*, 16(3), 321–333. DOI: https://doi.org/10.1177/1548512917707077
- Sécurité publique Canada. (2018) [s.d.] *National Cybersecurity Action Plan 2019-2024*. Récupéré de : https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf
- Singer, P.W., et Friedman, A. (2014) *Cybersecurity and Cyberwar: What everyone needs to know*, New York, Oxford University Press, 2014.
- Sudres, A. (2017). Cyberespace et dimension stratégique de la force informatique. *Stratégique*, (4) 117, 65-82. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0065
- Sur, S. (2004). Le conseil de sécurité : blocage, renouveau et avenir. *Pouvoirs*, 109(2), p.61-74. https://doi.org/10.3917/pouv.109.0061
- Shen, M. (2019, 29 juin) *China's Cyber Warfare Strategy and Approaches toward Taiwan*. Récupéré de : https://www.pf.org.tw/files/6510/A73CE07D-0D72-4AF8-9075-98A1CB188DA1
- Statista. [s.d.] *Countries with the highest military spending worldwide in 2020*. Récupéré de : https://www.statista.com/statistics/262742/countries-with-the-highest-military-spending/
- Statista. [s.d.] *Proposed federal spending by the U.S. government on cyber security for selected government agencies from FY 2020 to FY 2021*. Récupéré de : https://www.statista.com/statistics/737504/us-fed-gov-it-cyber-security-fy-budget/
- Statista. [s.d.] *Value of expenditure towards cyber security in India in 2019 with a forecast for 2022, by sector*. Récupéré de : https://www.statista.com/statistics/1099728/india-expenditure-towards-cyber-security-by-sector/
- UNIDIR. (2011) *Cyber Warfare and International Law : Ideas for Peace and Security*. Récupéré en ligne de : https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf
- UNIDIR. [s.d.] *The United Nations Institute for Disarmament research*. Récupéré de : https://unidir.org/
- UNODC. [s.d.] *Cyber warfare*. Récupéré de : https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberwarfare.html
- UNODC. (2014, mars) *Utilisation d'Internet à des fins terroristes*. [Rapport] https://www.unodc.org/documents/terrorism/Publications/The_Use_of_Internet_for_Terrorist_Purposes/Use_of_the_Internet_for_Terrorist_Purposes_French.pdf
- UNODC. [s.d.] *The United Nations Office on Drugs and Crime*. Récupéré de : https://www.unodc.org/
- United States' Department of Defense. (2021) [s.d.] *Program Acquisition Cost by Weapon System*. Récupéré de : https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2022/FY2022_Weapons.pdf
- United States' Department of Defense. (2021) [s.d.] *DOD Releases Fiscal Year 2021 Budget Proposal*. Récupéré de :

https://www.defense.gov/Newsroom/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/

- United States Naval Institute. (2021) [s.d.] *Russian Cyber Units*. Récupéré de : https://news.usni.org/2021/01/05/report-on-russian-cyber-units
- Talihärm, A. (2013) Towards Cyberpeace: Managing Cyberwar Through International Cooperation. *UN Chronicle*, 50 (2), 7-9.
- Taillat, S. (2017). L'impact du numérique sur les relations stratégiques internationales. *Stratégique*, 4 (117), 137-153. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0137
- Valeriano, B., et Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, 51(3), 347–360. DOI: https://doi.org/10.1177/0022343313518940
- Villani, C. (2019). Les enjeux de l'IA pour la Défense de demain. *Revue Défense Nationale*, 5 (820), 23-29. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/rdna.820.0023
- Weber, C. et Weber, J. (2017). La place de l'homme dans les enjeux de cybersécurité. *Stratégique*, (4) 117, 83-98. DOI: https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/strat.117.0083
- Yancey, Cyril K. (2019). Cyber Security: China and Russia's Erosion of 21st Century United States' Hegemony. *McNair Scholars Research Journal*, 12 (1) , Article 9. Récupéré de : https://commons.emich.edu/cgi/viewcontent.cgi?article=1147&context=mcnair
- Wilson, C. (2015, 4 juin) Cyber Weapons : 4 defining characteristics. *GCN*. https://gcn.com/articles/2015/06/04/cyber-weapon.aspx