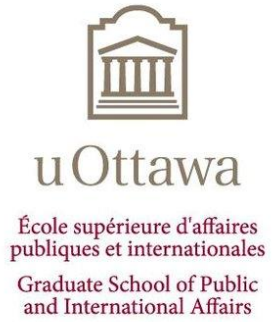
Félix Rioux

L’évolution stratégique de l’OTAN à l’épreuve du cyberespace

Mémoire soumis afin de satisfaire aux exigences

du programme de maîtrise en affaires publiques et internationales

Sous la supervision de la Professeure Costanza Musu



École supérieure d’affaires publiques et internationales

Université d’Ottawa

Le 17 mars 2021

Résumé

À l'ère de la révolution numérique, l'OTAN tarde à révéler une cyber-stratégie qui puisse efficacement répondre à la diversité des cyberattaques atteignant ses États membres au quotidien. Lors de la dernière décennie, l'Alliance atlantique a démontré une prise de conscience des menaces du cyberespace par le développement rapide de ses ressources cyber-défensives, la création de départements spécialisés et un regain de collaborations entre l'ensemble des États et parties alliés. Pourtant, le nombre de cyberattaques sur ses membres n'ont pas cessées de croître. Face à l'impuissance de la communauté internationale, qui peine à exercer le droit international sur les particularités modernes du cyberespace, l'OTAN est forcée de concevoir une nouvelle approche plus agressive à la défense de ses intérêts. À l'image de la stratégie de certains États, l'emphase est mise sur la dissuasion par l'emploi de cyberattaques contre-offensives envers ses détracteurs. Cependant, l'OTAN est encore loin d'avoir établi la régulation et l'opérabilité nécessaire pour en faire l'usage de manière unifiée et dans le respect des normes internationales.

Ce travail de recherche vise à décortiquer la cyber-stratégie de l'OTAN ainsi qu'à éclairer l'impact de ses intentions offensives sur la scène internationale. Par l'étude des stratégies nationales de ses membres et de ses plus grands rivaux, ce travail encadrera l'ambiance globale des politiques et des frictions qui continuent d'influencer le développement de sa stratégie. Enfin, la recherche exposera les défis internes et internationaux que l'Alliance devra surmonter afin d'obtenir une opérabilité cyber-offensive responsable et unifiée entre ses membres, et certaines solutions seront suggérées.

Table des matières

« Les États ont conclu qu'ils sont de plus en plus préoccupés par les implications de l'utilisation malveillante des TIC pour le maintien de la paix et de la sécurité internationale, et par la suite pour les droits de l'homme et le développement. »[1] [Traduction libre]

-Assemblée générale des Nations Unies,

Le 10 mars 2021

1 – Introduction

Depuis sa création en 1949, l'Organisation du traité de l'Atlantique nord (OTAN) a fait sa force par l'unification des ressources militaires de ses États membres et par sa déclaration de « défense collective », où une attaque contre l'un de ses membres serait considérée comme une attaque contre tous ses membres. L'utilisation dorénavant indispensable du cyberespace pour toute société contemporaine a à l'encontre introduit de tous les nouveaux défis sécuritaires pour ses États membres. Le cybercrime est en hausse d'année en année[2] [3], tout comme les actes de cyber-agression d'un État sur un autre[4].

[1] *Open-ended working group on developments in the field of information and telecommunications in the context of international security (A/AC.290/2021/CRP.2)*, United Nations, Le 10 mars 2021, file:///C:/Users/F%C3%A9lix/Downloads/Final-report-A-AC.290-2021-CRP.2.pdf : 3

[2] James Andrew Lewis, *Economic Impact of Cybercrime*, Center for Strategic and International Studies, le 21 février 2018, Economic Impact of Cybercrime | Center for Strategic and International Studies (csis.org)

[3] Tonya Riley, *The Cybersecurity 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds*, The Washington Post, Le 7 décembre 2020, The Cybersecurity 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds - The Washington Post

[4] Mohan B. Gazula, *Cyber Warfare Conflict Analysis and Case Studies*, Massachusetts Institute of Technology, Juin 2017, https://web.mit.edu/smadnick/www/wp/2017-10.pdf : 21

Afin de remédier aux cyberattaques qui atteignent les intérêts économiques et politiques de ses membres, de considérables efforts cyber-sécuritaires ont été produits par l'Organisation atlantique au cours de la dernière décennie. L'emphase générale de la stratégie a été mise sur la résilience, encourageant la coopération de ses membres et la fortification de leurs réseaux[5].

Face à l'incessante augmentation des cyberattaques, et ce même sur les réseaux fortement protégés, une nouvelle tactique globale s'installe. À l'image de la stratégie récente de certains de ses membres, l'OTAN souhaite se doter d'un pouvoir cyber-offensif pour potentiellement contre-attaquer les sources de cyberattaques s'acharnant sur les intérêts de l'un des leurs[6].

Ce travail de recherche a pour objectif de répondre à certaines questions en rapport avec la cyber-stratégie de l'OTAN. À quoi ressemble la cyber-stratégie présente de l'Alliance atlantique? Que manque-t-il à l'OTAN pour atteindre une force cyber-offensive unifiée? Quels sont les enjeux internes de l'implantation d'une force cyber-offensive, et quelles sont les considérations à prendre à l'externe de l'Alliance?

L'environnement du cyberespace révolutionne la manière dont les États mènent leurs conflits. Les nations rivales se penchent aujourd'hui vers la globalité de l'Internet pour s'ingérer dans les affaires des autres. Les particularités du cyberespace, permettant notamment aux acteurs de

[5] *Engagement en faveur de la cyberdéfense*, Organisation du traité de l'Atlantique nord, OTAN, Le 8 juillet 2016, NATO - Official text: Cyber Defence Pledge, 08-Jul.-2016

[6] *Remarks*, Organisation du traité de l'Atlantique nord, NATO - Opinion: Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London, 23-May.-2019

dissimuler l'origine de leur cyberattaque, laissent la communauté internationale majoritairement sans réponse sur la manière d'agir. Cette incertitude d'attribution et le manque de consensus international sur la définition des différents types d'agressions du cyberespace portent entrave à toute tentative d'un processus juridique et de l'application formelle de sanctions contre les États fautifs[7].

En l'absence d'un contrôle international, la cyber-stratégie de l'OTAN se transforme. L'Alliance laisse de plus en plus entrevoir qu'elle ne restera pas défensive et passive face aux enjeux du cyberespace. Depuis quelques années déjà, les membres de l'OTAN reconnaissent que la clause de défense collective couverte dans l'Article 5 du traité s'appliquerait tout autant aux actions portées dans cet environnement[8]. Toutefois, la grande majorité des cyberattaques, bien que parfois très dommageables, ne sont pas perçues comme des actes de guerre qui pourraient justifier un engagement militaire et l'application de l'Article 5. Néanmoins, une stratégie de dissuasion semble être envisagée.

Pour le moment, toutes ressources cyber-offensives restent dans les mains des autorités nationales de ses membres[9]. Il est à la discrétion des pays membres possédant leurs propres ressources cyber-offensives de venir en aide à un allié qui serait victime d'une cyberattaque lorsque le besoin de

[7] Lorraine Finlay et Christian Payne, *Why international law is failing to keep pace with technology in preventing cyber attacks*, The Conversation, Le 19 février 2019, https://theconversation.com/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks-111998
[8] *Cyberdéfense*, Organisation du traité de l'Atlantique nord, Le 20 octobre 2020, https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=fr
[9] Sophie Arts, *Offense as the New Defense: New Life for NATO's Cyber Policy*, The German Marshall Fund of the United States, nº 39, 2018, file:///C:/Users/F%C3%A9lix/Downloads/Offense%20-%20Arts.pdf : 5

contre-attaquer serait jugé nécessaire. L'OTAN n'a pour l'instant très peu de pouvoirs de coordination sur les opérations cyber-offensives et un État membre n'a aucune garantie sur le genre de support qu'un pays allié lui fournirait en cas de cyber-attaque importante.

Face aux cybermenaces d'aujourd'hui, une telle absence d'opérabilité unifiée reste largement insatisfaisante pour une alliance qui a longtemps fait sa force par une forte coordination des ressources militaires de ses membres. Ce manque de centralisation pourrait s'avérer incapacitant en temps de crise dû aux délais engendrés par la séparation générale des ressources disponibles et le manque de coordination stratégique[10].

En 2018, l'Alliance initie la création du Centre des opérations du cyberespace (*Cyberspace Operations Centre*), planifié d'être fonctionnel d'ici 2023, afin de permettre une meilleure coordination des capacités cybers de ses membres[11]. Ce département s'amène comme une forte indication des intentions futures de l'Alliance atlantique, mais plusieurs questions se posent toujours quant aux précisions de la stratégie et aux étapes pour atteindre une opérabilité unifiée. Pour y arriver, ses États membres devront rapidement s'entendre sur les définitions, les normes et les stratégies du cyberespace sur lesquelles toute opération d'un tel département se basera pour prendre ses décisions. Ce consensus devra de plus se faire en tenant compte des points de vue des

[10] Marios Panagiotis Efthymiopoulos, *A cyber-security framework for development, defense and innovation at NATO*, Journal of Innovation and Entrepreneurship, Vol. 8, nº 1, 2019, (PDF) A cyber-security framework for development, defense and innovation at NATO (researchgate.net) : 16

[11] Theodor Benien, *NATO's New Cyber Operations Centre*, Military Technology, mars 2020, Vol. 44, nº 5, p.34, https://www.monch.com/mpg/ebooks/military-technology/2020/05trya8lb/36/#zoom=z

grands acteurs internationaux, qui ne peuvent être ignorés dans l'élaboration d'une stratégie dissuasive qui aurait le potentiel d'enflammer des tensions internationales.

Pour le moment, la position officielle de l'OTAN reste encrée sous un angle défensif, puisant son utilité dans la résilience et l'assistance de ses États membres. Cependant, plusieurs indices semblent indiquer que la stratégie ne restera pas ainsi. Les aspirations offensives de l'Organisation atlantique présentent plusieurs obstacles. Afin de répondre à ces questions, j'introduirai tout d'abord les développements récents au sein de l'Alliance qui lui ont permis d'atteindre une forte résilience en termes de cybersécurité. J'encadrerai ensuite l'ambiance internationale des politiques du cyberespace et l'évolution des stratégies nationales en observant l'approche stratégique de certains de ses membres majeurs ainsi que certains de ses plus grands opposants. J'aborderai la transition de la stratégie de l'OTAN et je déterminerai enfin les obstacles internes et externes qu'elle devra résoudre afin d'atteindre certains de ses objectifs stratégiques souhaités, et en y formulant certaines solutions.

2- La stratégie de l'OTAN

La dernière décennie a naturellement été la plus marquante pour l'OTAN dans le développement d'une cyber-stratégie apte à contrer les cybermenaces de plus en plus présentes. Au travers de plusieurs rencontres entre ses États membres, l'OTAN a démontré qu'elle comprenait le besoin

immédiat d'améliorer sa stratégie et d'entreprendre des changements en réponse aux menaces modernes.

2.1 Les efforts cyber-sécuritaires de la dernière décennie

En 2012, au sommet de Chicago, l'OTAN affirme l'importance d'une approche de « défensive intelligente » qui implique la collaboration des États membres dans l'accomplissement de ses tâches fondamentales. Cet angle d'approche sera le fondement de la stratégie cyber-défensive de l'OTAN dans les nouveaux enjeux technologiques et informatiques qu'elle reconnaît à ce même sommet. Le sommet des Pays de Galles, en 2014, a apporté une plus grande attention sur les dangers des cyberattaques pour l'Alliance, qui établit la cybersécurité comme l'une de ses tâches fondamentales à soutenir et intensifie leur collaboration avec les industries privées de cybersécurité[12]. Il est confirmé aussi entre les membres lors de ce sommet que les lois sur le droit international telles que décrites par l'ONU s'appliquent également au cyberespace[13].

En 2016, au Sommet de Varsovie, les membres de l'OTAN s'entendent pour inclure la cybersécurité comme un environnement compris dans les domaines à défendre par l'Alliance au même titre que la terre, la mer et l'air (la reconnaissance de l'espace comme cinquième

[12] *NATO Cyber Defense*, North Atlantic Treaty Organization, NATO, Juillet 2016, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf
[13] *Déclaration du sommet du Pays de Galles*, Organisation du traité de l'Atlantique nord, Le 5 septembre 2014, NATO - Official text: Déclaration du sommet du Pays de Galles publiée par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue au pays de Galles, 05-Sep.-2014

environnement protégeable s'en suivra en 2019[14])[15]. À cette même année, l'OTAN s'engage pour avancer et supporter l'amélioration des réseaux de ses États membres en termes de cybersécurité[16]. Cet engagement implique une vision communautaire d'entraide et de résilience déclarant notamment que « Notre interconnectivité implique que nous ne sommes jamais plus fort que notre maillon le plus faible »[17].

Précédemment, en 2008, le Centre d'excellence de cyberdéfense coopérative de l'OTAN (*NATO Cooperative Cyber Defence Centre of Excellence*) est créé à Tallinn suivant la suggestion de l'Estonie dans l'objectif d'encourager une meilleure coopération des membres en termes de cybersécurité[18]. Ce centre fut un pas important pour l'Alliance, qui est depuis responsable de mener des recherches sur tous aspects de cybersécurité, en plus de former, d'entraîner et d'éduquer les départements de cyberdéfense des pays membres.

Les recherches du Centre ont mené, entre autres, à la création du Manuel de Tallinn, document rédigé par une collectivité de professionnels de renommée et dirigé par le professeur Michael N. Schmitt, président du *Naval War College* aux États-Unis. Publié en 2013, ce document avait pour but de fournir des lignes directrices de la manière dont le droit international devrait être appliqué et compris en situation de cyber-conflits. Une deuxième version du Manuel de Tallinn, le Manuel

[14] *Approche de l'OTAN concernant l'espace*, Organisation du traité de l'Atlantique nord, Le 27 octobre 2020, NATO - Topic: NATO's approach to space
[15] Bruno Lété, Daiga Dege, *NATO Cybersecurity: A Roadmap to Resilience*, The German Marshall Fund of the United States, Le 1 juillet 2017, NATO Cybersecurity: on JSTOR (uottawa.ca) : 2
[16] *Cyberdéfence*, Organisation du traité de l'Atlantique nord, Le 20 octobre 2020, NATO - Cyber defence
[17] *Engagement en faveur de la cyberdéfense*, Organisation du traité de l'Atlantique nord, OTAN, Le 8 juillet 2016, NATO - Official text: Cyber Defence Pledge, 08-Jul.-2016
[18] NATO CCDCOE, *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, [Vidéo], Youtube, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) - YouTube

de Tallinn 2.0, est publiée en 2017, mettant alors à jour les sujets véhiculés dans la première version et étend ses études à des cas potentiels de cyberguerres de plus grande envergure. Ces manuels sont souvent considérés comme la meilleure référence de ce que serait l'application du droit international aux les cyber-conflits et sont couramment référés par les créateurs de politiques civiles et militaires. Cependant, ce guide n'est pas officiellement souscrit dans les politiques de l'OTAN et ne représente pas sa position officielle[19]. L'OTAN ne reconnaît pas présentement de guide officiel concernant les actions d'agressions dans le cyberespace, mais retient les Manuels de Tallinn comme principales références. Il est important de noter que les Nations Unies n'ont pas non plus de tel guide en ce qui a trait aux cyber-agressions. Ce manquement à la communauté internationale rend alors difficile pour les pays de l'Alliance de s'entendre et de comprendre les mesures à prendre lors de situations précaires dans le cyberespace.

2.2 La résilience comme pilier stratégique

L'OTAN a été créée pour des raisons défensives. Depuis sa naissance, elle a participé à quelques opérations dans l'intention de défendre des populations contre possiblement de graves crimes de guerre sur le territoire européen, comme en Bosnie et au Kosovo, ainsi que sur des territoires étrangers, notamment en Libye, suivant l'approbation du Conseil de sécurité des Nations Unies.

Sa position défensive s'est efficacement transmise au cyberespace dans l'adoption d'une stratégie de « défensive intelligente » au Sommet de Chicago. Dans cette optique, l'OTAN entreprend de

[19] Oriane Barat-Ginies, *Existe-t-il un droit international du cyberespace?*, Hérodote, Vol. 1, nº 152-153, 2014, file:///C:/Users/F%C3%A9lix/Downloads/HER_152_0201.pdf : 202

nombreuses démarches internes pour assurer la sécurité de ses infrastructures[20]. Par l'entremise du Centre d'excellence de cyberdéfense coopérative de l'OTAN (CECCO), l'Alliance a pu amorcer l'amélioration des réseaux de tous ses pays membres, par l'échange de notions importantes concernant la cybersécurité, l'entraînement d'équipes d'experts nationales et par l'organisation d'exercices pratiques afin de mettre au défi leurs systèmes et le personnel en cybersécurité. En 2016, les chefs d'État des pays membres de l'OTAN se sont engagés à respecter les recommandations de l'Alliance visant l'amélioration de la protection de leurs réseaux. Ainsi, chacun s'engagera à mettre davantage d'efforts dans la sécurisation de leurs réseaux et infrastructures internes de manière à faire avancer le progrès défensif et à assurer une protection sur l'étendue des membres. Aussi, l'OTAN s'est doté d'équipes de réaction rapide disponibles en tout temps qui sont en mesure d'assister les pays membres qui se verraient victime d'une cyberattaque[21].

De plus, une collaboration plus étroite avec le secteur privé a été encouragée, qui tient aujourd'hui une place d'importance dans l'innovation des technologies du cyberespace[22]. Le secteur de l'industrie innove continuellement dans les technologies informatiques et ses contributions sont essentielles aux outils de protection de l'Alliance. Le recrutement de jeunes professionnels en cybersécurité peut s'avérer un défi pour le secteur public qui n'a souvent pas les ressources pour rivaliser avec les salaires offerts par les compagnies privées[23]. Leur collaboration est alors une

[20] *Défense intelligente*, Organisation du traité de l'Atlantique nord, Le 30 mars 2017, NATO - Topic: Smart Defence
[21] *Cyberdéfence*, Organisation du traité de l'Atlantique nord, Le 20 octobre 2020, NATO - Cyber defence
[22] *Three NATO Industry Cyber Partnership agreements signed at NIAS'19*, NATO Communications and Information Agency, Le 17 octobre 2019, NCI Agency | Three NATO Industry Cyber Partnership agreements signed at NIAS'19
[23] *Germany launches cybersecurity agency to strengthen 'digital sovereignty'*, DW, Le 8 novembre, 2020, https://www.dw.com/en/germany-launches-cybersecurity-agency-to-strengthen-digital-sovereignty/a-54529134#:~:text=The%20German%20government%20has%20signed,cyberthreats%20to%20the%20country's%20security

manière d'assurer d'être à jour sur toutes les plus récentes connaissances informatiques et cyber-sécuritaires.

Pour l'instant, l'emphase est mise sur la résilience. La résilience implique l'anticipation et la préparation de l'OTAN à rencontrer des menaces informatiques de tout genre. La défense collective, la gestion de crise et la sécurité coopérative sont trois tâches principales que s'est imposées l'Alliance lors de ses sommets afin de fortifier son objectif de résilience[24]. La demande pour une stratégie synergique et efficace deviendra d'autant plus importante dans les années à venir, par la multiplication des acteurs aux ressources capables de s'attaquer aux intérêts de ses États membres. La défensive intelligente par la résilience demande alors d'entreprendre des actions aujourd'hui pour se préparer contre les dangers de demain, ainsi que la perpétuation de la recherche sur les technologies émergentes pouvant être utilisées contre les intérêts de l'Alliance atlantique.

La stratégie de résilience implique aussi l'avancement et la solidification de relations avec d'autres organisations internationales. La relation entre l'OTAN et l'Union européenne date officiellement du début des années 2000, notamment par la Politique européenne de sécurité et de défense (PSED) en 2002[25]. En 2016, leur relation s'accentue en remédiant conjointement sur les défis actuels auxquels ils sont confrontés, dont les menaces hybrides et le terrorisme. Ces deux organisations, qui ont présentement 22 États membres en commun, se sont formellement entendues en 2018 lors

[24] Marios Panagiotis Efthymiopoulos, *A cyber-security framework*: 12
[25] *Relations avec l'Union européenne*, Organisation du traité de l'Atlantique nord, Le 31 juillet 2020, https://www.nato.int/cps/fr/natohq/topics_49217.htm

d'un sommet à Bruxelles sur la coopération des deux alliances dans le développement de capacités défensives, qui seront cohérentes et complémentaires.

Le groupe *Five Eyes* (ou de son abréviation *FVEY*) est une alliance entre les services de renseignements du Canada, du Royaume-Uni, de l'Australie, de la Nouvelle-Zélande et des États-Unis. Depuis ses origines des années suivant la Seconde Guerre mondiale, cette alliance profite d'une forte liaison unie par la confiance entre ces États aux valeurs similaires et usant d'une langue commune[26] [27]. Il s'agit en effet d'une relation qui peut être parfois difficilement réplicable dans des alliances comptant beaucoup plus de membres, comme l'OTAN, où la méfiance causera que certaines informations ne seront parfois pas partagées librement entre tous ses membres. Les avancées technologiques sur l'Internet, notamment l'avancée du réseau 5G chinois et la montée des confrontations des pays du *FVEY* avec la Chine et la Russie, assurent l'importance de cette collaboration dans leurs efforts et dans l'échange de renseignements[28]. Le Canada, le Royaume-Uni et les États-Unis étant à la fois membres du *FVEY* et de l'OTAN, il est sous-entendu qu'il existe un certain échange entre ces deux alliances, mais peu d'information à ce sujet est divulguée dans le domaine public.

[26] Greg Fyffe, *Should the Five Eyes Alliance be Expanded?*, Centre for International Policy Studies, Le 19 octobre 2020, https://www.cips-cepi.ca/2020/10/19/should-the-five-eyes-alliance-be-expanded/
[27] Jason Hanna, What is the Five Eyes intelligence pact?, CNN, Le 26 mai 2017, https://www.cnn.com/2017/05/25/world/uk-us-five-eyes-intelligence-explainer/index.html
[28] Heather Stewart, Mike Pompeo praises UK decision to remove Huawei from 5G network, The Guardian, Le 21 juillet 2020, https://www.theguardian.com/us-news/2020/jul/21/mike-pompeo-praises-uk-decision-to-remove-huawei-from-5g-network

Grâce à l'application et à l'innovation continuelle de ses mesures, il est généralement reconnu aujourd'hui que l'OTAN est bien préparée à se défendre contre des cyberattaques[29]. L'étendue des partenaires nationaux et internationaux, militaires et civiles, permet une résilience plus solide qu'aucun pays ne pourrait se doter par lui-même. Tout comme l'avantage que permet l'OTAN sur les forces traditionnelles, une telle collaboration accorde aussi aux pays membres des économies d'échelle sur les coûts normalement associés à l'acquisition d'une telle protection militaire contre les cybermenaces[30]. L'utilité et la pertinence de l'OTAN ne sont pas remises en doute.

Pourtant, malgré une préparation défensive adéquate par la résilience, les cyberattaques sur les infrastructures de l'OTAN ne cessent d'augmenter. Pour Michel Braud, « Une stratégie purement défensive reviendrait à construire une ligne Maginot du XXIe siècle »[31]. L'Organisation de l'Atlantique et ses membres n'en sont pas naïfs. Pour les pirates informatiques, les outils purement défensifs qui protègent les infrastructures dans le cyberespace ne constituent que des obstacles à contourner, des défis pour les adversaires les plus futés et munis des malwares informatiques à la fine pointe de la technologie. La course entre les avancements cyber-offensifs et cyber-défensifs n'aboutira semblablement jamais. C'est pour cette raison que plusieurs pays membres de l'OTAN ont déjà depuis quelques années démontrées le désir de développer une approche davantage offensive dans le cyberespace. Ceci n'est pas un secret pour l'Alliance. Le secrétaire général de l'OTAN, Jens Stoltenberg, a déjà mentionné la détermination de l'Alliance de ne pas rester

[29] Marios Panagiotis Efthymiopoulos, *op.cit.*: 8
[30] *Ibid.*: 12
[31] Michel Baud, *La cyberguerre n'aura pas lieu, mais il faut s'y préparer*, Institut français des relations internationales, Vol. 2, 2012, file:///C:/Users/F%C3%A9lix/Downloads/PE_122_0305%20(1).pdf : 305

purement défensive[32]. La résilience par la défense collective, la gestion efficace de crises et la sécurité coopérative au travers d'ententes à multiples niveaux est en effet un fier outil défensif pour le moment, mais n'avance pas une stratégie compréhensive pour ses membres face à l'évolution des défis envisageables.

Certains principaux acteurs nationaux au sein de l'OTAN ont apporté quelques changements dans leur plus récente stratégie de cybersécurité, déclenchant ainsi une tendance vers une approche plus offensive en réponse aux actes de cyber-agression. L'évolution de la stratégie de l'Alliance est inévitablement largement influencée par la posture cyber-stratégique officielle de ses membres. Il est également nécessaire de porter un regard sur les intentions des pays qui posent aujourd'hui les plus grandes menaces aux membres de l'OTAN afin de mieux comprendre les motivations de se diriger vers une stratégie plus combative.

2.3 Les positions adverses

Chine

La Chine est aujourd'hui une des plus grandes puissances économiques du monde. Selon les experts, elle devrait nettement réduire son écart économique avec les États-Unis dans les années à venir[33]. Comme toute puissance mondiale, la Chine est hautement interreliée à sa technologie. Pourtant, l'ouverture que permet l'Internet est à l'encontre en partie perçue comme une menace

[32] Patrick Tucker, *NATO Getting More Aggressive on Offensive Cyber*, Defense One, Le 24 mai 2019, NATO Getting More Aggressive on Offensive Cyber - Defense One
[33] Frédéric Lemaître, *La Chine, bulldozer de la croissance mondiale*, LeMonde, Le 12 janvier 2021, https://www.lemonde.fr/economie/article/2021/01/12/la-chine-bulldozer-de-la-croissance-mondiale_6065927_3234.html

pour le régime chinois, pour qui les influences externes et la liberté de l'information sont des risques à l'autorité du régime. En conséquence, le Grand Firewall de Chine a été mis en place pour censurer l'accès à certains sites et pour limiter le trafic externe sur les réseaux du pays[34]. Malgré son acceptation en 2013 que la Charte du droit international des Nations Unies s'appliquerait aux activités du cyberespace, le Parti communiste chinois (PCC) de Xi Jinping a maintes fois exprimé son intérêt de faire en sorte que l'Internet soit majoritairement régulé par les pouvoirs nationaux de chaque État[35]. Depuis les années 1990, les stratégistes chinois ont établi que le cyberespace pourrait offrir à la Chine une alternative efficace pour combler son écart de forces militaires traditionnelles avec d'autres puissances mondiales, principalement les États-Unis[36] [37]. En 1999, le livre « *Unrestricted Warfare* », sous son titre anglais, rédigé par deux colonels de l'Armée populaire de libération (APL), met de l'avant-plan la pensée stratégique de l'APL et du PCC en soutenant que l'avenir de la guerre se passerait au travers de d'autres sphères que la force militaire traditionnelle. Pour eux, la Chine atteindrait plus rapidement un avantage sur ses adversaires par l'amélioration de ses cyber-armes[38]. Le PCC est aujourd'hui soupçonné d'être derrière plusieurs cyberattaques récentes, principalement aux fins d'obtenir des avantages économiques sur ses adversaires[39] ou de promouvoir les valeurs du régime internationalement[40]. Plusieurs compagnies chinoises sont intimement liées au PCC et sont soupçonnées de fournir des informations

[34] Frédérick Douzet, *L'art de la guerre revisité. Cyberstratégie et cybermenace chinoises*, La Découverte, nº152-153, 2014, file:///C:/Users/F%C3%A9lix/Downloads/HER_152_0161.pdf : 163
[35] Mikk Raud, *China and Cyber: Attitudes, Strategies, Organisation*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf : 7
[36] Sophie Boisseau du Rocher, Emmanuel Dubois de Prisque, *La Chine e(s)t le monde : essai sur la sino-mondialisation*, Odile Jacob, Paris, Janvier 2019 : 190
[37] Mikk Raud, *op. cit.*: 9
[38] *Ibid.*: 9
[39] *Une cyberattaque chinoise stoppée avant que 900 000 entreprises en soient victimes*, Radio-Canada, Le 7 février 2019, https://ici.radio-canada.ca/nouvelle/1151627/chine-piratage-apt10-visma-attaque-infonuagique
[40] L'Australie se dit victime d'une cyberattaque d'un « acteur étatique », LaPresse, Le 18 juin 2020, https://www.lapresse.ca/international/asie-et-oceanie/2020-06-18/l-australie-se-dit-victime-d-une-cyberattaque-d-un-acteur-etatique

directement au régime. Un de ces exemples serait l'entreprise de technologies de communications Huawei[41]. En plus de cyberattaques, la Chine est fortement engagée dans l'espionnage, la collecte d'information sur les populations adverses et le vol de propriété intellectuelle[42] [43]. Un de ces cas importants a été le vol des plans de l'avion de chasse F-35 appartenant aux Américains. Tel qu'attendu, une version très similaire chinoise, nommée J-20, a été dévoilé quelques années après en 2016 par l'armée chinoise[44] [45]. Ce genre de perturbations sert aussi beaucoup aux compagnies privées chinoises et continuera de faire avancer le développement des domaines intellectuels et financiers du pays.

Russie

Bien que la Chine reste un adversaire de taille économiquement, la Russie représente pour plusieurs la plus grande menace à l'intégrité nationale et à la sécurité de ses citoyens dans le cyberespace. L'usage de cyberattaques par la Russie dans les deux dernières décennies, mais aussi leur immixtion remarquée dans les sphères informationnelles et les médias sociaux, s'intègrent dans une nouvelle stratégie militaire qui met en valeur le rôle des tactiques non violentes que permet l'Internet avec comme objectif l'affaiblissement des structures gouvernementales et sociales adverses[46]. Cette stratégie sous-entend non seulement l'espionnage et la recherche de

[41] Nushrod Nurkulov, *New Cyber Strategy of China and the Altercation in the Field*, Journal of Political Science and Public Affairs, Le 6 novembre 2017, file:///C:/Users/F%C3%A9lix/Downloads/new-cyber-strategy-of-china-and-the-alterations-in-the-field-2332-0761-1000310.pdf : 3
[42] Tom Robertson, Simon Van Hoeve, *Offensive Shifts, Offensive Policies: Cybersecurity Trends in the Government-Private Sector Relationship*, Canadian Global Affairs Institut, Août 2019, Offensive Shifts, Offensive Policies: Cybersecurity Trends in the Government-Private Sector Relationship - Canadian Global Affairs Institute (cgai.ca)
[43] Sophie Arts, *op. cit.:* 3
[44] Siobhan Gorman, August Cole, Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, The Wall Street Journal, Le 21 avril 2009, https://www.wsj.com/articles/SB124027491029837401
[45] Mikk Raud, *op. cit.*: 5
[46] Bilyana Lilly, Joe Cheravitch, *The Past, Present, and Future of Russia's Cyber Strategy and Forces*, RAND Corporation, 2020, CyCon_2020_book.indd (ccdcoe.org) : 131

failles potentielles dans les réseaux informatiques opposés, mais aussi l'agitation et l'affaiblissement interne des sociétés visées[47]. Cet objectif est souvent poursuivi par des manières de perturbation plus subtiles de subversion, de campagnes de désinformation et de propagande, particulièrement sur les médias sociaux. La guerre de l'information représente pour le Ministère de la Défense russe une tactique en soi à l'avant-plan de leur stratégie dans le cyberespace[48]. Certains sous-entendent alors que cette approche de déstabilisation perpétuelle employée par les autorités russes, et ce même en temps de paix traditionnelle, serait une démonstration que la cyberguerre est déjà en cours[49]. La Russie opérerait alors habilement dans la limite de l'acceptable, permis par l'absence des lois internationales concrètes sur les activités du cyberespace, de manière à ne pas provoquer le déclenchement d'une guerre traditionnelle. La justification pour leur stratégie s'enligne avec la vision depuis longtemps promue par les autorités russes selon laquelle leur pays est dépeint comme étant continuellement assiégé par les menaces internes et externes[50]. Les pays membres de l'OTAN sont alors principalement vus comme la nouvelle menace pour la Russie, mais plus précisément pour le régime de Vladimir Poutine, qui en serait le premier à souffrir si l'influence de l'ouest parvenait à influencer l'opinion publique russe. Il est en effet vrai que certains des pays membres de l'OTAN, particulièrement les États-Unis, ont fait l'usage du cyberespace pour influencer des populations à agir selon leurs intérêts au cours des années récentes[51]. La Russie perçoit donc ses actions comme étant égales aux techniques employées par ses adversaires et se voit du coup dans son droit de se défendre contre de telles tactiques

[47] Rod Thornton, Marina Miron, *Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom*, Journal of Cyber Policy, Vol. 4, nº 2, 2019, untitled (uottawa.ca) : 258
[48] Bilyana Lilly, Joe Cheravitch, *op. cit.*: 133
[49] Rod Thornton, Marina Miron, *op. cit.*: 259
[50] Bilyana Lilly, Joe Cheravitch, *op. cit.*: 134
[51] Rod Thornton, Marina Miron, *op. cit.*: 260

d'influences[52]. Elle se permet alors de maintenir une posture nationale qui prône une stratégie défensive de cybersécurité, tout en allouant une justification de ses actions évidemment offensives, mais pour lesquelles les autorités russes n'en prennent que très rarement la responsabilité.

Iran

Depuis la découverte du ver informatique Stuxnet en 2010, l'Iran s'est davantage investi dans le développement de ses cyber-capacités, défensives et offensives[53]. Ce pays a été motivé principalement dans le but de rattraper certains rivaux, dont les États-Unis, l'Israël et l'Arabie Saoudite, dans ce domaine en émergence. Certaines peurs internes motivent également leur développement, dont l'impression que le manque d'emprise sur ses réseaux d'Internet pourrait permettre le développement de révoltes à l'image du Printemps arabe[54]. Le pouvoir de l'Iran dans le cyberespace n'est pas encore à la hauteur des plus grandes puissances, mais démontre un développement rapide et une audace dans l'utilisation de ses cyber-capacités. Ce développement a été remarqué par plusieurs cyberattaques attribuées à l'Iran, notamment la cyberattaque de 2012 sur la compagnie saoudienne Aramco Oil par un virus informatique dévastateur intitulé Shamoon[55]. Une nouvelle variante de Shamoon a ensuite refait surface contre la même compagnie et il est largement accepté que le gouvernement iranien serait encore une fois derrière l'attaque[56] [57].

[52] Bilyana Lilly, Joe Cheravitch, *op. cit.*: 135
[53] Tom Robertson, Simon Van Hoeve, *op. cit*.
[54] James Andrew Lewis, *op. cit.*
[55] Christian Henning Lahmann, *op. cit.*: 8
[56] Christian Henning Lahmann, *op. cit.*: 9
[57] Baudouin Eschapasse, *Nouvelle cyberattaque contre des géants pétroliers*, LePoint, Le 17 décembre 2017, https://www.lepoint.fr/high-tech-internet/l-arabie-saoudite-sous-le-feu-de-hackers-25-01-2017-2099955_47.php

Corée du Nord

La Corée du Nord a depuis l'époque de Kim Jong Il eut un intérêt de développer des capacités cyber-offensives, y voyant un avantage tactique à faibles coûts. Depuis, le régime emploie les cyberattaques pour deux principales raisons. La première, comme plusieurs autres pays, tient à promouvoir les valeurs nord-coréennes à l'étranger. Cette tactique a notamment été remarquée en 2014 par l'opération *Blockbuster*, une cyberattaque ciblée vers la compagnie *Sony Pictures Entertainement*[58]. Cette attaque est provenue de la Corée du Nord et aurait été lancée en réponse à la sortie du film *The Interview*, où l'histoire tourne autour d'une tentative d'assassinat de Kim Jong Un. Leur seconde intention principale dans le cyberespace provient de l'usage de cyberattaques à des gains financiers[59]. Le cyberespace permet au régime de contourner certaines sanctions qui leur sont imposées par la communauté internationale. Un vol de 81 millions de dollars de la Banque Centrale du Bangladesh a notamment été découvert et attribué à l'État nord-coréen. Cet usage est une particularité, car la majorité des États n'utilisent pas les cyberattaques comme source directe de revenus.

Les pays identifiés comme les plus grandes menaces à l'OTAN dans le cyberespace partagent tous la particularité que leur présence sur le web est tout autant importante dans l'affront de leurs adversaires internationaux à l'externe, que pour assurer le contrôle du régime au pouvoir à l'interne. Chacun de ces régimes respecte très peu les droits humains et accorde peu de tolérance

[58] Kong Ji Young, Lim Jong In, Kim Kyoung Gon, *The All-Purpose Sword: North Korea's Cyber Operations and Strategies*, NATO CCDCOE Publications, 2019, CyCon_2019_Kong_Kim_Lim.indd (ccdcoe.org) : 10
[59] Tom Robertson, Simon Van Hoeve, *op. cit.*

à la critique du régime, d'après les plus récents rapports d'Amnistie internationale[60]. L'OTAN s'oppose alors principalement à des régimes autoritaires qui ont le pouvoir d'agir librement sans aucune critique ou indignation permise de la part de leur population. Par l'absence de critiques internes, le poids et l'opinion de la communauté internationale pourraient être davantage importants à l'encadrement éthique et légal des actions pouvant être portées dans le cyberespace.

Il est majoritairement compris depuis quelques années que le droit international encadrant les activités des États s'applique tout autant aux activités dans le cyberespace[61]. Cependant, dû aux différences et aux innovations qu'apportent les outils de cet environnement, l'application de cette loi n'est souvent pas comprise universellement[62]. Au moment présent, l'OTAN ne peut pas seulement se fier au droit international pour défendre ses intérêts contre des cyberattaques. Une stratégie moderne, claire et unifiée sera cruciale afin d'accomplir son mandat défensif.

2.4 La stratégie des principaux États membres

États-Unis

En 2018, le département de la défense des États-Unis dévoile son plan de cyber-stratégie, dans lequel ils confirment leur intention d'utiliser des tactiques offensives lorsque nécessaire afin de

[60] Rapport Annuel 2019, Amnesty International, https://www.amnesty.be/infos/rapports-annuels/rapport-annuel-2019/
[61] Harold Hongju Koh, *International Law in Cyberspace*, Havard International Law Journal, Vol. 54, Décembre 2012, International Law in Cyberspace (yale.edu) : 3
[62] Cyrus Jabbari, *The Application of International Law in Cyberspace: State of Play*, Office of Disarmament Affairs, United Nations, 25 octobre 2018, https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/

promouvoir la dissuasion dans le cyberespace[63]. Le département emploie l'expression « *defending forward* », ou « défendre de l'avant », pour justifier leur intention d'agir anticipativement face à des menaces perçues dans le cyberespace. Ce nouvel angle offensif n'explique pas précisément quels genres d'opérations seront menées en « défendant de l'avant », ou même quels genres de menaces sont suffisantes pour entreprendre une action contre celles-ci. Le document fait d'ailleurs mention de la Chine et de la Russie comme les principaux adversaires aux intérêts américains dans le cyberespace. Le rapport met l'emphase sur la dissuasion comme stratégie d'approche, et amplifie sa crédibilité en confirmant que des actions seront prises contre ceux qui planifient nuire aux intérêts américains. Il ne cache pas non plus les intentions américaines de promouvoir leurs valeurs et intérêts dans le cyberespace. Le document se distingue de son prédécesseur de 2015, sous l'administration de Barack Obama, par une plus grande acceptation qu'il existe plusieurs risques et menaces à l'ouverture de l'Internet et que les Américains ne peuvent se permettre de rester passifs en défense de leurs intérêts. La stratégie d'atténuer les risques en 2015 est alors remplacée par la stratégie de défense active et plus agressive en 2018. La tentative d'ingérence dans les élections américaines par les Russes ainsi que la prolifération générale des crimes et des attentats dans le cyberespace contre les intérêts américains au fil des trois années qui ont séparé ces deux rapports stratégiques pourraient expliquer l'intensification de la stratégie.

L'intrusion la plus récente aux États-Unis dans le logiciel Orion à l'automne 2020 a poussé le président Joe Biden à déclarer qu'il ne resterait pas les bras croisés dans cette affaire et que son

[63] *2018 Department of Defense Cyber Strategy*, Department of Defense, United States of America, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF : 2

administration fera de la cybersécurité une priorité[64]. Cette déclaration laisse présager que la stratégie de défendre de l'avant fera tout autant partie de la stratégie cyber lors de la présidence de Biden, et pourrait même employer des tactiques plus agressives encore. La vision stratégique des États-Unis est évidemment d'importance pour l'OTAN, ayant les ressources technologiques militaires les plus avancées du monde[65] et étant son plus grand contributeur financier[66].

France

La France a également déclaré son intérêt d'adopter une approche plus offensive dans le cyberespace ainsi qu'en support aux campagnes militaires, tel qu'indiqué en 2019 par la ministre des Armées françaises, Florence Parly[67]. Tout comme les Américains, la France envisage continuer à miser sur la collaboration avec le secteur privé, ainsi qu'avec ses alliés pour continuellement renforcer ses capacités cybers.

[64] Andrew Solender, *'I Will Not Stand Idly By': Biden Says Cybersecurity Will Be 'Top Priority' After Giant Hack*, Forbes, Le 17 décembre 2020, https://www.forbes.com/sites/andrewsolender/2020/12/17/i-will-not-stand-idly-by-biden-says-cybersecurity-will-be-top-priority-after-giant-hack/?sh=412ac4705159

[65] *A new global ranking of cyber-power throws up some surprises*, The Economist, Le 17 septembre, 2020, https://www.economist.com/science-and-technology/2020/09/17/a-new-global-ranking-of-cyber-power-throws-up-some-surprises

[66] *Trump: What does the US contribute to Nato in Europe?*, BBC News, Le 30 juillet 2020, https://www.bbc.com/news/world-44717074#:~:text=The%20civilian%20and%20military%20budget,other%20members%20of%20the%20alliance

[67] *Communiqué_La France se dote d'une doctrine militaire offensive dans le cyberespace et renforce sa politique de lutte informatique défensive*., Ministère des armées, Le 18 janvier 2019, Communiqué_La France se dote d'une doctrine militaire offensive dans le cyberespace et renforce sa politique de lutte informatique défensive. (defense.gouv.fr)

Royaume-Uni

Avec le dévoilement de leur stratégie nationale dans le cyberespace en 2016, le Royaume-Uni se plaçait déjà à l'époque dans l'optique d'une stratégie défensive basée sur la dissuasion par la possibilité de riposte contre les instigateurs d'une attaque[68]. Le plan s'étendait sur 5 ans, soit jusqu'en 2021, et une nouvelle stratégie nationale devrait être divulguée prochainement. Le Brexit ne devrait pas avoir d'impact sur les relations du Royaume-Uni avec l'OTAN, même que certains estiment que cette séparation du Royaume-Uni avec l'Union européenne pourrait pousser un rapprochement avec l'Alliance par leur désir de retenir de fortes relations avec d'autres ententes en place[69].

Allemagne

En 2016, l'Allemagne aussi révèle son plan stratégique militaire par les « *White Papers* » de ses forces armées, la *Bundeswehr*[70]. Ce document marque pour l'Allemagne la reconnaissance du rôle militaire dans les enjeux du cyberespace, et les nouvelles tactiques auxquelles se méfier, dont les campagnes hybrides de désinformation et d'ingérence politique[71]. En 2018, l'Allemagne lance un nouveau département au coût de 350 millions d'euros entièrement destiné à l'amélioration de la

[68] *National Cyber Security Strategy 2016-2021*, HM Government, National Cyber Security Strategy 2016-2021 (publishing.service.gov.uk) : 47
[69] Naz Gocek, *Brexit's Impact on NATO and European Security*, Association Canadienne pour l'OTAN, LE 8 avril 2019, https://natoassociation.ca/brexits-impact-on-nato-and-european-security/
[70] *2016 White Paper on German Security Policy and the Future of the Bundeswehr*, The Federal Government, 2016, 2016-White-Paper-1.pdf (ccdcoe.org)
[71] Martin Schallbruch, Isabel Marie Skierka, *The Evolution of the German Cybersecurity Strategy*, Springer Briefs in Cybersecurity, Juillet 2018, file:///C:/Users/F%C3%A9lix/Downloads/CybersecurityinGermany_Manuscript_Chapter3%20(1).pdf : 9

coordination et la sécurité générale de ses réseaux[72]. L'Allemagne est restée majoritairement discrète quant à ses intentions cyber-offensives, mais a tout de même reconnu l'implication stratégique et militaire qui existe dorénavant dans le cyberespace et son importance au niveau étatique.

3- L'évolution de la stratégie : L'approche dissuasive

D'après leur plus récent rapport stratégique, les puissances de l'OTAN semblent toutes être majoritairement en accord avec l'approche sécuritaire à prendre afin d'assurer leur sécurité nationale. L'amélioration des systèmes défensifs, l'entraînement de personnel et la collaboration avec le secteur privé et les pays alliés sont bien évidemment fortement exprimés dans leur rapport, mais une récente emphase sur le pouvoir de dissuasion et les capacités offensives lorsque nécessaire semble aussi être avancée. Ceci marque une transition dans la tendance précédente des pays occidentaux de soutenir une position davantage défensive dans le cyberespace, du moins de ce qui était déclaré publiquement. Ce changement pourrait être attribué à la réalisation de l'ampleur que pourrait prendre le cyberespace dans les querelles étatiques, par la diversification des tactiques d'ingérence politique et économique qui ont été observées dans les années récentes. Certains pays,

[72] *Germany launches cybersecurity agency to strengthen 'digital sovereignty'*, DW, Le 8 novembre, 2020, https://www.dw.com/en/germany-launches-cybersecurity-agency-to-strengthen-digital-sovereignty/a-54529134#:~:text=The%20German%20government%20has%20signed,cyberthreats%20to%20the%20country's%20security

dont le Canada[73] [74], n'ont toutefois pas émis de plan visant à obtenir des fonctions nationales cyber-offensives, ou que leur utilisation demeure officiellement très restreinte. Il est compréhensible cependant que certains États membres de l'OTAN n'aient pas les capacités militaires ou économiques requises pour entreprendre une telle posture sur le cyberespace. Ces pays pourraient tout autant supporter un angle offensif pris par l'OTAN, en assistant l'Alliance par quelconques moyens à leur disposition.

En ligne avec la posture changeante des États, l'idéologie cyber-stratégique générale de l'OTAN a vu quelques transformations dans les années récentes. En 2018, l'Alliance dévoile la création d'un tout nouveau département entièrement dévoué à l'amélioration de ses cyber capacités qui sera en opération en 2023[75]. Ce dévoilement est alors en accord avec le besoin de l'heure d'accélérer le développement de la cybersécurité de l'Alliance pour contrer les dangers pressentis du cyberespace. Leur but : atteindre l'interopérabilité complète entre les pays membres de l'OTAN dans le domaine de la cybersécurité. Ce nouveau centre de commande opérable en 2023 sera érigé pour recevoir des renseignements militaires en temps réel et coordonner les actions de cyber-dissuasion de ses pays membres sous un seul toit[76]. Un tel département rendra sans aucun doute plus crédible le pouvoir de dissuasion de l'OTAN, qui permettra dorénavant une meilleure collaboration à la contre-attaque et une coordination plus efficace des opérations. Certains

[73] *Stratégie nationale de cybersécurité*, Sécurité publique Canada, Gouvernement du Canada, https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx
[74] Kathleen Harris, *Liberals to create 'super' national security watchdog as part of anti-terror law overhaul,* CBC News, Le 20 juin 2017, https://www.cbc.ca/news/politics/security-terrorism-legislation-1.4168780
[75] Robert Janczewski, Grzegorz Pilarski, Maciej Marczyk, *Terminology as a Barrier to NATO's Interoperability in Cyberspace Operations*, International Conference Knowledge-Based Organization, Warsaw, Vol. 25, nº 3, 2019, Terminology as a Barrier to NATO's Interoperability in Cyberspace Operations in: International conference KNOWLEDGE-BASED ORGANIZATION Volume 25 Issue 3 (2019) (sciendo.com) : 32
[76] Robin Emmott, *NATO cyber command to be fully operational in 2023*, Reuters, Le 16 octobre 2018, NATO cyber command to be fully operational in 2023 | Reuters

souhaitent même qu'un tel département puisse ouvrir la porte à la possibilité de conduire des opérations offensives entièrement sous un commandement de l'OTAN par l'unification des cyber-ressources de ses membres[77]. Néanmoins, des règles claires quant aux actions cyber-offensives que l'Alliance aurait le droit d'employer sont toujours absentes à la stratégie, dont quel type de cyberattaque sur un allié justifierait l'implication de la clause de défense collective de l'Article 5.

3.1 Les implications d'une stratégie de cyber-dissuasion

La prochaine étape de la stratégie de l'OTAN passera sans doute par le Centre des opérations du cyberespace, planifié d'être fonctionnel d'ici 2023. Ce centre constituera le point focal des cyber-capacités contre-offensives et offensives de l'Alliance et ainsi assurera son pouvoir de dissuasion. Toutefois, l'emploi d'actions cyber-offensives au nom d'un groupe d'États demande beaucoup plus de responsabilisation et de coopération au sein de l'Alliance que l'application de mesures seulement défensives. Les actions offensives sont réprimandables par la communauté internationale. Dans n'importe quel contexte politique ou stratégique, une grande opposition se formera quant à la nécessité et la moralité de s'engager dans des opérations offensives. Pourtant, les membres de l'OTAN semblent être d'accord que la dissuasion est aujourd'hui essentielle à une stratégie défensive pertinente. L'Alliance atlantique a traditionnellement fait sa force par la coordination et la collaboration de ses membres. Cette même interopérabilité doit également être présente pour ses opérations du cyberespace, sans quoi l'avantage que permet l'unification de leurs ressources militaires sera trop souvent freiné par des débats internes sur les actions à prendre. Une telle organisation est d'autant plus importante, car les décisions qui seront prises sur la manière de

[77] Robin Emmott, *op. cit.*

réagir à une cyberattaque pourraient avoir des conséquences internationales graves, qui doivent être bien comprises dans l'élaboration de la stratégie.

3.1.1 L'escalade de conflits

Dès lors que l'OTAN et certains de ses États membres d'importance ont déclaré qu'ils emploieraient la dissuasion comme tactique cyber-défensive, l'escalade de conflits mineurs et intermédiaires devient une inquiétude. Comme nous en sommes conscients, pour qu'une tactique de dissuasion soit efficace, elle doit être crédible. Pour qu'elle soit crédible, elle ne peut pas seulement reposer sur des menaces. Comme David J. Lonsdale l'explique, une stratégie de dissuasion ne peut être dissociée de la guerre, car son efficacité en dépend[78]. Une stratégie de cyber-dissuasion implique alors l'emploi éventuel de cyberattaques contre ceux qui auront commis une infraction contre nos intérêts. Il explique de plus que la dissuasion sans ressources et sans encadrement a le potentiel d'être perçue comme des menaces vides[79]. À l'encontre, se doter des ressources et d'un plan d'action concret rend les contre-mesures plus crédibles et convaincantes que la menace puisse en effet être livrée. Les cyberattaques contre l'OTAN et ses membres continuent d'augmenter année après année en partie parce que, bien que l'Alliance ait divulgué ses plans d'utiliser des contre-mesures, elle est encore loin logistiquement de pouvoir les administrer avec conviction. La préparation présente de l'Alliance suppose qu'en cas de cyberattaque, un des membres aux capabilités cyber-offensives devra se porter volontaire pour venir en aide et agir en défense d'un autre État membre.

[78] David J. Lonsdale, *op. cit.*: 410
[79] David J. Lonsdale, *op. cit.*: 417

Une stratégie de dissuasion concrète n'est toutefois pas imperméable. L'OTAN devra savoir quand et comment réagir de manière convaincante, mais responsable. Les contre-mesures apportent les risques d'aggraver les conflits. L'important pour l'Alliance sera de préalablement encadrer internationalement, comme à l'interne, les actions qui peuvent être posées. Elle devra s'assurer d'une législation et d'un mode d'emploi qui s'enlignent avec la Théorie de la guerre juste (*Just War Theory*), où la proportionnalité et la discrimination sont mises de l'avant pour minimiser les effets néfastes pour la population. Selon la Théorie de la guerre juste, les conflits doivent être engendrés seulement dans l'espoir que ses résultats procureront un meilleur futur. Comme le suggère le Manuel de Tallinn, les contre-mesures devraient être conduites contre la source de l'attaque et devraient pouvoir être annulées une fois que l'État ou l'organisation visée ait cessé ses agressions[80]. Ces mesures peuvent aussi être sous la forme de sanctions économiques ou politiques. Lorsque des contre-attaques cybers sont menées, elles devraient cibler majoritairement les ressources offensives de l'État afin de réduire leur pouvoir de représailles et elle devrait autant que possible éviter les effets sur les populations civiles.

3.1.2 Envisager des conséquences réalistes de la cyberguerre

La situation ne doit pourtant pas être dramatisée. Il est nécessaire ici de connaître les limites des enjeux du cyberespace pour prendre des décisions mieux éclairées sur les besoins futurs de l'OTAN. La culture populaire influencée par certains films hollywoodiens nous a fait craindre

[80] Michael N. Schmitt, et collab., *Tallinn Manuel on the International Law Applicable to Cyber Warfare*, Cambridge University Press, New York, 2013, 356296245.pdf (peacepalacelibrary.nl) : 36

qu'une cyberattaque puisse mettre à genoux un pays entier par les actions de quelques pirates informatiques indépendants. Difficile de croire qu'un tel scénario proviendrait d'acteurs indépendants dû aux types de renseignements privilégiés sur les infrastructures ciblées et aux ressources technologiques et pratiques nécessaires pour entreprendre une telle opération. En ce qui a trait aux menaces provenant d'un État adverse, le sujet est davantage débattu.

Tel que Sean Lawson l'a étudié dans son chapitre intitulé « *Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats* », les scénarios apocalyptiques sont couramment employés par les promoteurs de cybersécurité pour encadrer la problématique d'un angle qui viendra chercher des émotions et la peur de la population, qui ainsi acceptera d'investir davantage dans le domaine[81]. Cette idée est supportée par les travaux de Myriam Dunn Cavelty pour expliquer en quoi la dramatisation des scénarios d'attaque dans le cyberespace est basée sur des hypothèses qui n'ont jamais été réellement employées jusqu'à présent. Cette peur infondée a le potentiel de mener à la sécurisation du domaine[82]. Une telle sécurisation face aux menaces imaginées mène alors à la justification de certaines mesures normalement exceptionnelles, dont l'espionnage avancé des gouvernements sur leur propre population, qui semble aujourd'hui être une pratique courante. Pourtant, les cyberattaques qui ont été observées à ce jour sont loin d'être vu comme un scénario de destruction massive, ayant pour la plupart infligés que des perturbations momentanées et aucune conséquence directes menant à des pertes de vies[83].

[81] Sean Lawson, *Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats*, Routledge, Journal of information Technology and Politics, Vol. 10, 2013, C:\iTools\WMS\TandF-Journals\3833133\WorkingFolder\WITP_A_759059.dvi (uottawa.ca) : 86
[82] *Ibid.*: 88
[83] David J. Lonsdale, *op. cit.*: 418

L'auteur se réfère aux peurs exprimées au début du 20e siècle, à l'époque de plusieurs avancées technologiques, dont l'idée que le développement du bombardement aérien lors de conflits démontrerait la fragilité de l'interdépendance des villes à leur technologie. Pour les alarmistes de l'époque, de tels bombardements mèneraient au chaos total, détruisant les réseaux électriques des villes ciblées et effaçant tout ordre social. Lawson démontre toutefois que, lors de la Seconde Guerre mondiale, le Royaume-Uni, l'Allemagne et l'Italie ont en fait été capables d'augmenter leur production d'électricité malgré la destruction[84]. Même dans les pires cas de bombardement, dont le déploiement de la bombe nucléaire sur Hiroshima, les systèmes sociaux en place s'étaient montrés résilients. Les gens n'ont pas été paralysés par la dévastation comme nous aurions pu le croire, et ont maintenu la fonctionnalité des services urgents[85].

Cet exemple doit être pris en compte dans notre assomption que les cyberattaques auront des conséquences apocalyptiques sur les sociétés, sans aucune preuve empirique pour soutenir ces thèses. L'attaque sur l'Estonie en 2007 est parfois mentionnée comme l'un des plus marquants exemples d'une cyberattaque et le premier exemple d'une cyberguerre[86]. Pourtant, bien que cet évènement se soit déroulé à un moment où les systèmes de cybersécurité étaient encore peu développés, les dommages causés par la cyberattaque ont été pour la plupart seulement contraignants et temporaires. Aucune vie n'a été perdue[87].

[84] Sean Lawson, *op. cit.*: 92
[85] Sean Lawson, *op. cit.*: 92
[86] Laurent Zecchini, Olivier Truc, *Les cyberattaques massives d'origine russe contre l'Estonie préoccupent l'Alliance atlantique*, Le Monde, Le 26 mai 2008, https://www.lemonde.fr/europe/article/2007/05/19/les-cyberattaques-massives-d-origine-russe-contre-l-estonie-preoccupent-l-alliance-atlantique_912244_3214.html
[87] Michel Braud, *op. cit.*: 305

Il est important de retenir cependant que la société d'aujourd'hui est bien plus interreliée à sa technologie qu'elle ne l'était lors de la Seconde Guerre mondiale. Des cyberattaques qui auraient de plus grandes conséquences que celles vues en Estonie sont bien réelles et il est important de s'y préparer. L'OTAN doit envisager des scénarios réalistes, et non de vivre des peurs hypothétiques, afin d'appuyer une préparation plus adéquate face aux dangers plausibles et d'encourager des solutions constructives axées sur les enjeux présents.

4- Les défis d'une stratégie offensive

Tout en appliquant une conception réaliste des menaces du cyberespace, l'OTAN aura le devoir d'entrevoir certains obstacles qui se posent dans le chemin d'une opérabilité cyber-offensive unifiée. Elle ne pourra agir sans le consentement et l'implication de ses membres, et doit comprendre et respecter l'implication des parties internationales dans les actions qu'elle pourrait poser.

4.1 Les obstacles internes

L'arrivée de Donald J. Trump à la présidence américaine en 2016 a apporté des doutes quant à la direction que prendrait l'OTAN dans les années à venir. Le 45^{e} président des États-Unis aux discours et aux politiques isolationnistes avait très tôt fait savoir qu'il considérait que les Américains payaient une trop grande proportion envers l'OTAN et qu'il n'était pas intéressé à

dépenser autant de ressources dans la défense de leurs alliées[88]. Ces déclarations avaient alors mis en doute, pour certains, la pertinence même de l'Alliance atlantique[89], pour qui les États-Unis financent une grande part de son budget annuelle (22% du son budget total en 2019, et près de 8% de plus que l'Allemagne, le second plus grand contributeur)[90].

Heureusement pour l'OTAN, l'élection du démocrate Joe Biden à la présidence américaine à l'automne 2020 a tourné une page tumultueuse avec son plus grand contributeur financier. Biden se présente comme un fort supporteur de l'Alliance et devrait graduellement remettre les pendules à l'heure à l'avancement des buts sécuritaires communs. Le désengagement militaire américain initié par Trump pourrait tout de même se poursuivre sous l'administration Biden, mais l'OTAN pourra dépendre des États-Unis pour reprendre ses objectifs défensifs contre ses plus gros rivaux, notamment la Russie et la Chine. Ils pourront aussi adresser ensemble la question de la Turquie, un des États membres de l'OTAN, qui est responsable de certaines controverses à l'interne de l'Alliance dans les récentes années[91].

La diversité des États membres de l'OTAN peut en effet constituer un obstacle aux objectifs unifiés qu'elle tente d'avancer. Les relations de la Turquie avec l'Alliance atlantique ont été quelque peu

[88] Françoise Marmouyet, *Les pays de l'Otan face à l'isolationnisme version Donald Trump*, France24, Le 13 novembre 2016, https://www.france24.com/fr/20161111-donald-trump-otan-budget-europe-securite
[89] Gilles Vandal, *Une remise en question des alliances comme l'OTAN*, La Tribune numérique, Le 12 août 2018, https://www.latribune.ca/opinions/une-remise-en-question-des-alliances-comme-lotan-d808fa74d45d5112500771a43c54aa4f
[90] *Trump: What does the US contribute to Nato in Europe?*, BBC News, Le 30 juillet 2020, https://www.bbc.com/news/world-44717074#:~:text=The%20civilian%20and%20military%20budget,other%20members%20of%20the%20alliance
[91] Christian Spillmann, *L'OTAN classe les années Trump et attend Joe Biden*, LaPresse, Le 1 décembre 2020, https://www.lapresse.ca/international/europe/2020-12-01/l-otan-classe-les-annees-trump-et-attend-joe-biden.php

mouvementées récemment dû à certaines décisions venant de leur dirigeant controversé, Recep Tayyip Erdoğan. Les décisions de ce dernier sont parfois perçues comme étant à l'encontre des valeurs et des objectifs de l'OTAN, ce qui a créé de la discorde au sein des membres. Jens Stoltenberg a en effet précisé que la Turquie se permettait de bloquer plusieurs tentatives de partenariats de l'OTAN, à l'encontre de l'opinion générale des membres[92]. L'achat d'un système de défense anti-missile provenant de la Russie qui n'est pas opérable avec les systèmes de l'OTAN[93], en plus de tensions passées lors d'un incident en mer Méditerranée impliquant un navire français en mission pour l'OTAN[94], ne sont que quelques exemples des difficultés de l'Alliance avec son partenaire turc.

De telles mésententes et confrontations entre les États membres sont des obstacles attendus pour une organisation avec un grand nombre de membres lors de la planification d'opérations. Les avantages que procure l'Alliance ne font toutefois pas de doute et, malgré les mésententes engendrées par certaines administrations politiques, chacun des États comprend les bénéfices d'en faire partie. L'Alliance permet des économies d'échelles aux nations par le partage des coûts, des ressources et du renseignement[95]. Ces États profitent aussi, bien évidemment, d'une protection militaire plus complète et à multiples niveaux. Les plans d'avancer la défense et les capacités de l'Alliance dans le cyberespace ne sont que plus intéressantes pour ses membres qui s'inquiètent aujourd'hui de la protection de leurs réseaux dans cet environnement en continuelle expansion.

[92] Christian Spillmann, *op. cit.*
[93] *Ibid.*
[94] *L'OTAN ouvre une enquête sur l'incident entre la France et la Turquie en Méditerranée*, Le Monde, Le 18 juin 2020, https://www.lemonde.fr/international/article/2020/06/17/paris-denonce-une-man-uvre-turque-recente-extremement-agressive-en-mediterranee_6043175_3210.html
[95] Marios Panagiotis Efthymiopoulos, *op. cit.*: 12

Les sources de frictions entre membres ne devraient être que passagers, ayant chacun des intérêts importants à rester au sein de l'Alliance.

Malgré quelques fluctuations dans les dynamiques nationales internes, l'OTAN a encore beaucoup de chemin à faire afin de réduire les possibilités de conflits et de mésententes sur le plan pratique et opérationnel. En déterminant a priori certaines notions et stratégies d'emploi pratiques, les risques de mésententes sur la manière de mener des opérations contre-offensives unifiées seront nettement diminués. Mes recherches ont déterminé que trois points majeurs sont absents de la stratégie présente à l'interne de l'OTAN. L'Alliance devra tout d'abord définir un lexique commun pour les termes du cyberespace, ériger un guide d'actions concernant ses capacités contre-offensive et assurer un meilleur échange de renseignements entre ses membres ainsi qu'avec ses partenaires.

4.1.1 Définition des termes

Tel que Don Lewis, directeur adjoint du Centre des opérations du cyberespace, le mentionne, les menaces du cyberespace sont déjà très présentes et l'OTAN n'a de choix que de bâtir ses départements d'opération au fur et à mesure, sans connaître précisément ce qui s'en suivra[96]. Le chemin pour aboutir à l'interopérabilité efficace des ressources de ses membres n'est pas clairement identifié. Pourtant, certaines étapes peuvent être franchies graduellement qui faciliteront ensuite les suivantes. Une de ces étapes d'importance serait d'assurer que tous les

[96] Don Lewis, *What is NATO Really Doing in Cyberspace?*, War On the Rocks, Le 4 février 2019, What Is NATO Really Doing in Cyberspace? - War on the Rocks

membres ont la même compréhension des termes du cyberespace. Des chercheurs de l'Université de Varsovie ont identifié que l'OTAN n'a toujours pas élaboré un guide terminologique unifié pour les différents termes du cyberespace et des divergences existent dans le lexique de chaque nation[97]. Ils ont observé par exemple que les États membres de l'OTAN, notamment les États-Unis, l'Allemagne et la Pologne, ont des définitions différentes pour certains termes aussi généraux que le mot « cyberespace » dans leurs documents officiels. Il n'existe pas non plus de consensus sur les termes « cyberattaque » et « cyberdéfense ». Ceci augure mal lorsque l'Alliance considère qu'une cyberattaque importante pourrait justifier la défense collective et l'application de l'Article 5. De telles divergences dans la définition auraient le potentiel de nettement ralentir le processus décisif et la réactivité de l'Alliance lorsque ses membres seraient forcés d'évaluer si une cyberattaque subite doit être considérée importante et quel type de réponse serait adéquate. L'OTAN doit absolument établir certaines définitions qui seront comprises et incorporées sur l'ensemble des documents officiels de ses membres afin d'assurer la fluidité de sa prise de décision.

4.1.2 Améliorer l'échange

Présentement, les États membres restent en contrôle des ressources qu'ils fournissent à l'OTAN et toutes capacités de contre-mesures offensives demeurent à la discrétion du pays fournissant l'assistance. Par cette procédure, les commandants de l'Alliance devront demander une l'assistance auprès d'un pays pour employer une cyber-arme et le service serait fournis par le membre, sans devoir divulguer plus d'information[98]. Ceci pourrait largement limiter la prise de

[97] Robert Janczewski, Grzegorz Pilarski, Maciej Marczyk, *op. cit.*: 33
[98] Sophie Arts, *op. cit.*: 6

décision stratégique du Centre des opérations du cyberespace de l'OTAN, limitant ainsi son efficacité.

Une amélioration de l'échange demandera inévitablement une forte coopération américaine, qui est une des principales sources de renseignements de l'OTAN. L'augmentation du transfert d'information inquiète toutefois certains partis que les renseignements transmis pourraient être compromis dans les mains d'un membre avec une cybersécurité nationale inférieure[99]. L'OTAN aura le devoir d'assurer qu'un système fortement sécurisé soit mis en place, par lequel les États membres et les partenaires de l'Alliance seront en mesure de soumettre des renseignements secrets directement au centre de commande tactique. Les informations sensibles ne seraient pas divulguées avec le reste des membres. Un tel système d'échange d'information sera essentiel à son opérabilité stratégique.

4.1.3 Élaboration d'un guide

L'OTAN devra aussi se doter d'un guide d'action précis sur lequel se baseront toutes les décisions à prendre en réponse à des cyber-agressions sur un membre. Ce guide devra encadrer la prise de décision face à chaque cyber-agression contre un membre et déterminer ce qui sera permis d'employer comme mesures anticipatives contre un agresseur potentiel. Il sera crucial afin d'éviter des transgressions possibles de la part des commandants de l'OTAN et d'écarter les implications politiques nationales de la prise de décision. Il est à noter, cependant, que plusieurs membres souhaitent s'abstenir de divulguer un plan concret de réponse aux différents types de cyberattaques

[99] Sophie Arts, *op. cit.*: 6

par peur que leurs adversaires s'y réfèreront pour envoyer des attaques tout juste en dessous de ce que l'État ciblé considère grave[100]. Les détracteurs pourraient alors envoyer une cyberattaque importante, mais qui éviterait de peu une réponse militaire, ou se servir de plus petites cyber-agressions qui n'engendraient pas de réponses concrètes. Les adversaires pourraient alors précisément anticiper les conséquences de leurs actions. Ceci n'empêche pas toutefois qu'un guide puisse être érigé et gardé secret, au même titre que des informations sensibles militaires, et qu'il soit continuellement innové pour répondre aux menaces changeantes.

L'OTAN n'est pourtant pas sans ressources pour y répondre. Malgré qu'il ne soit présentement pas officiellement reconnu dans les démarches de l'Alliance, le Manuel de Tallinn et le Manuel de Tallin 2.0, érigés par des professionnels du domaine sous les instructions du Centre d'excellence de cyberdéfense coopérative de l'OTAN, pourraient en être une solution. Ces extraits représentent la conception la plus complète à ce jour de l'interprétation de la réglementation des conflits de la Charte des Nations Unies et du droit international humanitaire de la Croix Rouge dans le cyberespace. Ils offrent des précisions sur tous les concepts majeurs reliés aux droits des États et aux actes illégaux lors d'opérations dans le cyberespace. Certaines notions font toutefois exception dans ce texte, leur résolution ne faisant pas l'unanimité des experts, et leur réponse est laissée ouverte. Une révision finale de ces documents serait donc nécessaire. Ce guide pourrait servir d'une grande source d'inspiration pour s'accorder sur les démarches à suivre en cas de cyberattaque.

[100] Sophie Arts, *op. cit.*: 2

Selon la Charte de Nations Unies, l'OTAN ne pourrait qu'employer des capacités cyber-offensives sous l'autorisation du Conseil de sécurité ou en guise de légitime défense pour l'un de ses membres qui serait victime d'une cyber-agression majeure[101]. Le Manuel de Tallinn indique cependant que l'OTAN serait en effet dans ses droits de riposter collectivement contre un agresseur commettant une offense sur l'un de ses membres, car elle représente une alliance ayant précédemment conclu un accord de défense collective[102]. Cela étant dit, seule une cyberattaque importante engendrait une telle permission selon la loi présente. Bien entendu, il serait difficile aujourd'hui d'avoir une seule définition pour une cyberattaque qui pourrait justifier cette permission. Les auteurs du Manuel suggèrent plutôt que l'attaque soit évaluée d'après sa sévérité, son immédiateté, sa cause à effet, son degré d'invasion dans le système ciblé, l'évaluation des effets, son caractère militaire, le niveau d'implication d'un État, et la présomption de la légalité[103]. Développés en détail dans le Manuel, ces critères sont une ressource adéquate, et en accord avec le principe international de *Jus ad Bellum,* sur lesquels les États membres pourraient objectivement évaluer l'action à prendre.

Le Manuel de Tallinn permet de plus l'emploi de « contre-mesures » proportionnelles, via sa Règle 9[104], en accord avec certains Articles du Projet d'articles sur la responsabilité de l'État pour fait international illicite des Nations Unies (2001)[105]. C'est bien d'après cette Règle que l'OTAN serait en mesure de justifier sa stratégie de dissuasion face à des cyberattaques sur ses infrastructures. Ces contre-mesures doivent tout de même être en réponse à un acte illégal selon le droit

[101] *La Charte des Nations Unies*, Chapitre 7, Article 51, 1945, Chapter VII | Nations Unies
[102]Michael N. Schmitt et collab., *op. cit.*: 67
[103] Michael N. Schmitt et collab., *op. cit.*: 48
[104] Ibid.: 36
[105] *Projet d'articles sur la responsabilité de l'État pour fait international illicite*, Nations Unies, 2001, https://legal.un.org/ilc/texts/instruments/french/draft_articles/9_6_2001.pdf

international, ce qui exclurait par exemple de riposter contre des actes de cyber-espionnage. Les contre-mesures doivent être proportionnelles aux dommages causés par la cyberattaque initiale et être employées dans l'objectif d'induire la partie fautive à corriger ses transgressions et à respecter les exigences du droit international[106]. Les experts ayant écrit le Manuel de Tallinn ne se sont toutefois pas entendu si des contre-mesures punitives, soit même après que l'agression initiale eut cessée, pourraient être employées. Voici ici un cas où l'OTAN devrait préciser ses intentions. Il semblerait pourtant que la tactique présente de dissuasion de certains pays membres de l'OTAN insinuerait que des mesures punitives après les faits seraient acceptables selon eux.

En référence avec la plus récente cyberattaque contre les États-Unis en automne 2020, en exemple, il doit tout d'abord être déterminé si l'on parle effectivement ici d'une cyberattaque qui motiverait une riposte. Plusieurs ont suggéré que l'attaque sur le système d'Orion de la compagnie SolarWinds avait plus les allures d'une opération de cyber-espionnage que d'une attaque destructrice contre les infrastructures américaines[107]. Dans tous les cas, les Américains ont les outils nécessaires pour décider du plan d'action en réponse à cette cyberattaque, sans avoir recours directement aux services des autres pays membres de l'OTAN. Si cette même cyberattaque s'était déroulée sur un autre pays membre moins puissant, toutefois, l'Alliance serait dans l'obligation de déterminer la méthode adéquate d'action selon un plan établi.

[106]Michael N. Schmitt et collab., *op. cit.*: 37
[107] *US cyber-attack: US energy department confirms it was hit by Sunburst hack*, BBC News, Le 18 décembre 2020, https://www.bbc.com/news/world-us-canada-55358332

Chaque exemple de cyberattaque contre les membres de l'OTAN apporte ses propres particularités, souvent sans précédent sur la manière de réagir. L'OTAN se doit d'adopter des lignes directrices précédemment établies dans le but de limiter les débats et les désaccords entre membres lors de situations urgentes et précaires. La diversité des membres de l'Alliance s'avère souvent un atout à sa force, mais peut aussi engendrer des défauts à son opérabilité.

En plus de définir les termes importants, de permettre un système d'échange de renseignements rapide et discret et d'élaborer les lignes directrices des réponses aux cyberattaques, l'Alliance devra clairement identifier la chaîne de commandement lorsque de contre-mesures doivent être utilisées. Les exercices pratiques de simulations de cyberattaques en temps réel, par l'entremise du Centre d'excellence de cyberdéfense coopérative de l'OTAN, sont une excellente manière d'assurer la compréhension du rôle de chacun et d'entraîner la réactivité générale de l'Alliance.

4.2 Obstacles à l'international

L'un des plus grands obstacles au contrôle des cyber-agressions est son manque de régulation, mais aussi son manque de définition sur la scène internationale[108]. En 2013, le Groupe d'experts gouvernementaux représentant la vision de l'ONU a publié un rapport qui confirme définitivement que les règles existantes du droit international s'appliquaient également aux actions des États dans le cyberespace[109] [110]. Ceci assure à tous qu'il existe des limites aux actions pouvant être portées

[108]Sean Lawson, *op. cit.*: 97
[109] Julien Nocetti, *Géopolitique de la cyber-conflictualité*, Politique étrangère, Vol. 2, 2018, Géopolitique de la cyber-conflictualité | Cairn.info (uottawa.ca) : 25
[110] Harriet Moynihan, *The Application of International Law to State Cyberattacks, Sovereignty and Non-intervention*, The Royal Institute of International Affairs, Décembre 2019, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf: 6

via le web contre une nation adverse et que des sanctions pourraient être imposées en cas d'agression grave, selon les principes évoqués dans la Charte des Nations Unies. Dans le contexte moderne et innovateur des technologies du cyberespace, toutefois, cette interprétation n'encadre pas efficacement les particularités distinctes de cet environnement virtuel. Ceci résulte à une compréhension nettement incomplète de la Charte. Ces manques de précision au droit international, où il n'existe pas de mesures proprement adaptées aux particularités du cyberespace, entravent à toute médiation des cyber-conflits et encouragent les États à régler leurs comptes par des actions qu'ils jugeront eux-mêmes adéquates.

À l'encontre, l'encadrement des cyber-conflits par l'élaboration de normes internationales du cyberespace devrait améliorer la confiance entre États, encourager la discussion, et aurait le pouvoir d'éviter l'aggravation de conflits liés à des mésententes[111]. Il sera utile notamment pour l'OTAN, dans son objectif potentiel d'obtenir une force centralisée aux capacités offensives, d'encourager le développement d'une clarification du droit international sur les actions du cyberespace qui serait en mesure de correctement encadrer les cyber-transgressions.

Les Conventions de Genève et le droit humanitaire international ont eu dans l'histoire moderne l'effet de limiter les conséquences de la guerre sur les populations civiles. Au contraire de l'encadrement international de la guerre cinétique traditionnelle, qui a profité d'une forte compassion médiatique à la vue de ses actes de violences, les dangers du cyberespace inquiètent

[111] Nicolay Akatyev, Joshua I. James, *Legislative Requirements for Cyber Peacekeeping*, Journal of Digital Forensics, Security and Law, Vol. 12, n° 3, Article 4, Octobre 2017, https://commons-erau-edu.proxy.bib.uottawa.ca/jdfsl/vol12/iss3/4/ : 27

généralement moins les populations[112]. Bien qu'elles ne fassent pas de victimes directes, ses conséquences ont le potentiel d'atteindre beaucoup plus de personnes et de causer des dommages collatéraux imprévisibles. Si une cyberguerre était déclenchée, des effets pires encore pourraient affecter les populations civiles, par des cyberattaques ciblant des infrastructures essentielles, dont par exemple des usines de traitement d'eau.

Les puissances mondiales reconnaissent les dangers de la cyberguerre et l'utilité du développement d'un droit international lié aux particularités de cet environnement. Les Nations Unies rassemblent régulièrement des délégués d'État pour échanger sur de grandes questions se rapportant aux technologies de l'information et de la communication (TIC). Ces rencontres permettent de clarifiés certains sujets et incitent les États à adhérer à certaines normes non-contraignantes du cyberespace dans le but d'anticiper certains enjeux qui risquent de créer des conflits et d'éviter les mésententes[113]. Ces discussions sont d'importance dans l'objectif de prévenir les excédents du cyberespace de la part des États. La création d'un droit international contraignant du cyberespace est toutefois difficilement envisageable dans l'environnement politique international présent. Deux obstacles majeurs empêchent une telle constitution : la problématique de l'attribution et les idéologies divergentes sur le contrôle de l'Internet.

[112] Jorge Barbosa, *Cyber Humanity in Cyber War*, European Conference on Cyber Warfare and Security, Juin 2020, Cyber Humanity in Cyber War - ProQuest (uottawa.ca) : 22

[113] *Open-ended working group on developments in the field of information and telecommunications in the context of international security (A/AC.290/2021/CRP.2)*, United Nations, Le 10 mars 2021, file:///C:/Users/F%C3%A9lix/Downloads/Final-report-A-AC.290-2021-CRP.2.pdf : 4

4.2.1 La problématique de l'attribution

Dans le cyberespace, non seulement est-il possible d'efficacement dissimuler la provenance réelle d'une cyberattaque, les actions illicites par un État sont très rarement directement déployées par des départements gouvernementaux officiels[114]. Il s'avère bien plus sécuritaire pour les gouvernements de mandater des groupes externes pour mener ce type d'opération. Ceci leur donne ainsi la possibilité de démentir toute accusation d'implication étatique si l'attaque est retracée jusqu'aux serveurs du pays. Tout organe international tentant de médier à un conflit suivant une cyberattaque ne pourrait pas trancher avec certitude sur les auteurs exacts et des sanctions seraient difficilement attribuables. De plus, bien que des suspicions peuvent être déclarées dès la découverte de l'attaque, l'enquête professionnelle pour en découvrir l'origine peut durer plusieurs mois[115]. Des recherches ont aussi découvert que les entités victimes d'une cyberattaque prennent en moyenne 200 jours avant même d'être au courant que leurs infrastructures ont été compromises[116]. Ces lourds délais sont davantage encombrants dans la rectitude de toute dispute, où l'État victime serait sans doute pressé de venger l'agression. Dans la plupart des cas, l'enquête ne serait qu'en mesure de situer la provenance régionale de la cyberattaque, sans pouvoir fermement déterminer si l'État était impliqué dans son élaboration. Selon le droit international, l'État n'est pas responsable des agissements d'acteurs indépendants si elle n'en est pas associée directement, et ce, même s'ils résident sur son territoire[117]. Toute médiation internationale se verrait donc complexe et débattable.

---

[114] Julien Nocetti, *op. cit.*: 20
[115]Christian Henning Lahmann, *op. cit.*: 15
[116] *Ibid.*
[117] *International Law Commission, Articles on State Responsibility*, United Nations International Law Commission, Le 10 août 2001, https://casebook.icrc.org/case-study/international-law-commission-articles-state-responsibility#:~:text=Article%208&text=The%20conduct%20of%20a%20person%20or%20group%20of%20persons%20shall,in%20carrying%20out%20the%20conduct : Article 8

Cet obstacle d'attribution peut aussi encombrer l'Alliance atlantique dans sa tactique cyber-offensive. Si l'OTAN souhaite faire l'usage de contre-mesures, elle devra concevoir qu'elle opérera souvent avec un degré d'incertitude sur l'identité réelle de ses agresseurs. Elle devra agir sans doute sans l'approbation formelle de la communauté internationale, advenant qu'un traité quelconque soit conclu, qui aurait certainement ses propres doutes à porter des accusations contre un État.

4.2.2 Accords internationaux difficiles

La conclusion d'un accord du droit international du cyberespace reste improbable aujourd'hui dû au clivage existant entre deux points de vue majeurs sur la régulation du le cyberespace. Les États-Unis, et supporté par ses alliés membres de l'OTAN, ont toujours promu le cyberespace comme un environnement ouvert, où la liberté d'expression est soutenue et où le contrôle gouvernemental devrait rester minimal[118]. À l'encontre, les pays dont la Chine et la Russie, et supportés au travers de l'Organisation de coopération de Shanghai (OCS), ont affirmé leur désir d'une délimitation plus marquée du pouvoir souverain des États sur le web. Cette dernière stratégie s'avère avantageuse aux régimes autoritaires qui souhaitent avoir un contrôle plus accru sur leur réseau interne et de limiter l'ingérence extérieure. En ce sens, les pays membres de l'OTAN sont plutôt en faveur que le cyberespace soit régulé par une entité internationale, tandis que la majorité des membres de l'OCS seraient en faveur que les États restent en plein contrôle de leur réseau interne[119].

[118] Nicolay Akatyev, *op. cit.*: 27
[119] *Ibid*.: 29

Les nations sont toutefois très au courant des dangers que puissent accorder un cyber-conflit et présentent certains efforts afin d'éviter l'escalade de conflits. Les discussions organisées par l'ONU, invitant la participation de représentants de chaque pays dans but de clarifier certains débats sur les termes du cyberespace, pourraient être la solution la plus appropriée pour le moment.

En revanche, sans l'appui officiel de puissants États dont la Chine et la Russie, il serait difficile d'envisager qu'une entente concrète sur le droit international du cyberespace et qu'une entité régulatrice puisse être créés. L'incapacité d'attribuer avec certitude les États coupables d'une cyberattaque et le clivage existant entre les perceptions des États de l'ouest et de l'est sur la manière de réguler le cyberespace semblent représenter des obstacles insurmontables pour le moment présent. Néanmoins, continuer les efforts de définitions des termes du cyberespace représentant les points de vue des supporteurs de chaque idéologie par la discussion s'avérera essentiel à la conciliation d'une structure mondiale aussi divisée.

Pour l'OTAN, la clarification des termes du cyberespace à l'international lui permettra de mieux défendre ses intérêts en tentant de s'entendre avec les autres puissances sur certaines cibles et certaines actions inacceptables du cyberespace. Elle pourra mieux comprendre les intérêts et les inquiétudes des autres États, ce qui assurera que ses tactiques contre-offensives employées n'auront pas des conséquences qui pourraient escalader un conflit démesurément. Grâce à ces discussions, elle pourra ériger une stratégie défensive et un plan d'action qui seront davantage axés sur la protection des intérêts qui n'auront pas été résolus lors de ces rencontres. Bien entendu, ces

discussions ne contraignent aucun État et ne garantiront pas sa sécurité sur les intérêts couverts, mais peuvent être extrêmement bénéfiques à la stabilité du cyberespace par la délimitation de certaines actions aux conséquences graves et par la réduction des mésententes.

Conclusion

À l'ère du XXIe siècle, la pertinence de l'OTAN a retrouvé un souffle dans le rôle capital qu'elle jouera face aux menaces du cyberespace. La hausse des cyberattaques de la dernière décennie a poussé l'Alliance à réagir rapidement. Par un objectif de résilience et une stratégie de défensive intelligente, où les systèmes cyber-défensifs de chacun des membres ont été améliorés et une forte collaboration est encouragée au travers des parties alliées, l'OTAN assure à ses membres une fière protection en termes de cybersécurité. Pourtant, les cyberattaques évoluent, et leur nombre ne cesse d'augmenter. Celles plus subtiles et innovantes observées au cours des dernières années semblent indiquer qu'une stratégie purement défensive ne sera pas suffisante face aux dangers évolutifs du cyberespace. À l'image de la transformation de la stratégie de ses États membres au niveau national, l'Alliance semble démontrer un intérêt à supporter, et même mener, des opérations contre-offensive, ne restant pas seulement défensive et réactive. La création du Centre des opérations du cyberespace sera un tremplin pour l'avancement de cet angle offensif.

Nous avons cependant remarqué que plusieurs obstacles doivent toujours être franchis afin d'atteindre une telle opérabilité. À l'interne, les membres de l'OTAN devraient tout d'abord

établir des définitions pour les termes importants du cyberespace qui seront introduits dans les stratégies nationales de chaque État. L'Alliance devra améliorer ses pratiques communicationnelles afin d'encourager l'échange de renseignements importants, avec discrétion et sécurité. Il sera crucial enfin, dans le but d'obtenir une opérabilité sur des actions cyber-offensives, d'officiellement adopter un guide opérationnel basé sur des lois et des normes acceptées par tous et en respect du droit international existant. Si ces obstacles ne sont pas surmontés, l'opérabilité et l'efficacité de l'Alliance souffriront de la pluralité de ses membres et s'enfargeront continuellement sur des désaccords politiques et bureaucratiques. À l'externe, les difficultés d'établir un droit international s'appliquant efficacement au cyberespace posent un problème que l'Alliance ne pourrait régler d'elle-même. Son engagement dans les discussions constructives avec les puissances mondiales sur certaines des grandes questions cyber-sécuritaires devrait continuer d'être encouragé. Les frictions avec la vision chinoise et russe sur le rôle des États dans le cyberespace continueront de faire entrave à l'élaboration d'un droit international universel, mais les discussions avec ces opposants devraient limiter l'escalade de conflits mineurs.

Une coordination stratégique entre ses États et avec ses partenaires pourrait s'avérer plus cruciale encore face aux technologies qui façonneront le futur du cyberespace. L'implication de l'Intelligence artificielle (IA) dans l'avenir des fonctions cybers défensives et offensives s'avère la voie révolutionnaire des technologies informatiques. Une course au développement de cette technologie est déjà en cours. Les États savent que ceux qui gagneront cette course obtiendront

un atout considérable à leur stratégie de dissuasion[120]. L'Alliance ne peut seulement miser sur des investissements financiers pour développer cette technologie, elle doit de plus miser sur une forte coordination avec ses partenaires et pleinement profiter des avantages comparatifs entre ses membres. Tel que l'indique Rob Murray, chef de l'Unité Innovation de la Division Défis de sécurité émergents de l'OTAN : « Les pays qui remporteront cette course seront peut-être d'ailleurs ceux qui possèdent la bureaucratie la plus agile et non ceux qui auront développé les meilleures technologies »[121].

L'évolution de l'OTAN doit continuer d'impliquer une vision davantage unifiée pour rivaliser avec les puissances opposées qui gagnent rapidement en pouvoir et en prospérité. Cette vision doit être appliquée tant au niveau international qu'avec le secteur privé et académique. La force de l'OTAN provient de sa pluralité et de sa diversité. Ces atouts apportent une résilience efficace lorsque appliqués en cybersécurité. Elles donnent un poids considérable à son pouvoir dissuasif et seront indispensables à sa force cyber-offensive. Dans l'avenir, cette collaboration étroite continuera de stimuler l'innovation qui assurera la protection de ses États membres au sein d'un monde davantage informatisé et virtuel.

[120] Rob Murray, *L'Alliance a tout intérêt à se doter d'une filière d'innovation résiliente*, NATO Review, Le 1 septembre 2020, L'Alliance a tout intérêt à se doter d'une filière d'innovation résiliente (nato.int)
[121] Rob Murray, *op. cit.*

Bibliographie

AGENCE FRANCE-PRESSE. « *L'Australie se dit victime d'une cyberattaque d'un 'acteur étatique'* », *LaPresse*, [En ligne], Le 18 juin 2020, [https://www.lapresse.ca/international/asie-et-oceanie/2020-06-18/l-australie-se-dit-victime-d-une-cyberattaque-d-un-acteur-etatique] (page consultée le 19 janvier 2021)

AGENCE FRANCE-PRESSE. « Les États-Unis lancent des cyberattaques sur l'EI », *LaPresse*, [En ligne], Le 26 avril 2016, [https://www.lapresse.ca/international/dossiers/le-groupe-etat-islamique/201604/26/01-4975272-les-etats-unis-lancent-des-cyberattaques-sur-lei.php] (page consultée le 4 janvier 2021)

AKATYEV, Nicolay, et I. JAMES, Joshua. « Legislative Requirements for Cyber Peacekeeping », *Journal of Digital Forensics, Security and Law*, Vol. 12, nº 3, Article 4, 2017, p.23-38. DOI: https://doi.org/10.15394/jdfsl.2017.1447

AKOTO, Evelyne. « Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public? : Première partie », *Revue de droit d'Ottawa*, Vol. 46, nº1, 2015, 23 pages. [Page 1 - Page 10 | Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : Première partie | CanLII] (page consultée le 15 décembre 2020)

AMENSTY INTERNATIONAL. « Rapport Annuel 2019 », *Amnesty International*, [En ligne], [https://www.amnesty.be/infos/rapports-annuels/rapport-annuel-2019/] (page consultée le 18 janvier 2021)

ARTS, Sophie. « Offense as the New Defense: New Life for NATO's Cyber Policy », *The German Marshall Fund of the United States*, nº 39, 2018, 9 pages. [file:///C:/Users/F%C3%A9lix/Downloads/Offense%20-%20Arts.pdf] (page consultée le 3 février 2021)

BARAT-GINIES, Oriane. *« Existe-t-il un droit international du cyberespace? »*, *Hérodote*, Vol. 1, nº 152-153, 2014, p.201-220. [Existe-t-il un droit international du cyberespace ? | Cairn.info](page consultée le 8 février 2021)

BARBOSA, Jorge. « Cyber Humanity in Cyber War », *European Conference on Cyber Warfare and Security*, 2020, 7 pages. DOI:10.34190/EWS.20.116

BBC NEWS. « Trump: What does the US contribute to Nato in Europe? », *BBC News*, [En ligne], Le 30 juillet 2020, [https://www.bbc.com/news/world-44717074#:~:text=The%20civilian%20and%20military%20budget,other%20members%20of%20the%20alliance](page consultée le 11 janvier 2021)

BBC NEWS. « Trump: What does the US contribute to Nato in Europe? », *BBC News*, [En ligne], Le 30 juillet 2020, [https://www.bbc.com/news/world-44717074#:~:text=The%20civilian%20and%20military%20budget,other%20members%20of%20the%20alliance](page consultée le 7 janvier 2021)

BBC NEWS. « US cyber-attack: US energy department confirms it was hit by Sunburst hack », *BBC News*, [En ligne], Le 18 décembre 2020, [https://www.bbc.com/news/world-us-canada-55358332] (Page consultée le 10 février 2021)

BENIEN, Theodor. « NATO's New Cyber Operations Centre », *Military Technology*, [En ligne], Vol. 44, nº 5, mars 2020, p.34-35. [https://www.monch.com/mpg/ebooks/military-technology/2020/05trya8lb/36/#zoom=z] (page consultée le 1 mars 2021)

BERCUSON J., David. « NATO: Past, Present and Future », *Canadian Global Affairs Institute*, [En ligne], 2019, [NATO: Past, Present and Future - Canadian Global Affairs Institute (cgai.ca)] (page consultée le 29 décembre 2020)

BOISSEAU DU ROCHER, Sophie, et DUBOIS DE PRISQUE, Emmanuel. *La Chine e(s)t le monde : essai sur la sino-mondialisation*, Paris, Odile Jacob, 2019, 295 p.

BRAUD, Michel. « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Institut français des relations internationales*, Vol. 2, 2012, p.305-316. [La cyberguerre n'aura pas lieu, mais il faut s'y préparer | Cairn.info](page consultée le 1 février 2021)

BREENE, Keith. « Who are the cyberwar superpowers? », *World Economic Forum*, [En ligne], Le 4 mai 2016, [Who are the cyberwar superpowers? | World Economic Forum (weforum.org)](page consultee le 22 décembre 2020)

BREWSTER, Murray. « As Britain reveals its first-ever cyberattack against ISIS, experts ask if Canada will be as open », *CBC*, [En ligne], Le 19 mai 2018, [https://www.cbc.ca/news/politics/britain-canada-cyber-attack-notice-1.4669710](page consultée le 4 janvier 2021)

BRITANNICA, « Stuxnet Computer Worm », *Britannica*, [En ligne], Mise à jour le 23 novembre 2016. [https://www.britannica.com/technology/Stuxnet] (page consultée le 11 janvier 2021)

BROCKMEIER, Sarah, et STUENKEL, Oliver, et TOURINHO, Marcos. « The Impact of the Libya Intervention Debates on Norms of Protection », *Global Society*, Vol. 30, nº1, 2016, p.113-133. doi:10.1080/13600826.2015.1094029.

BRONK, Chris, et S. ANDERSON, Gregory. « Encounter Battle: Engaging ISIL in Cyberspace », *The Cyber Defense Review*, Vol. 2, No. 1, 2017, p.93-108. [https://www.jstor.org/stable/26267403]

CENTER FOR STRATEGIC AND INTERNATION STUDIES. « Significant Cyber Incidents Since 2006 », *Center for Strategic and International Studies*, [En ligne], [https://csis-website-prod.s3.amazonaws.com/s3fs-public/210129_Significant_Cyber_Events.pdf] (page consultée le 24 janvier 2021)

CERULUS, Laurens. « SolarWinds is 'largest' cyberattack ever, Microsoft president says », *Politico*, [En ligne], Le 15 février 2021, [SolarWinds is 'largest' cyberattack ever, Microsoft president says – POLITICO] (page consultée le 19 février 2021)

CREVIER, Alain. « Le monde est tellement (moins) violent », *Radio-Canada*, [En ligne], Le 18 janvier 2018, [https://ici.radio-canada.ca/nouvelle/1147407/alain-crevier-steven-pinker-monde-violence] (page consultée le 22 décembre 2020)

DOUZET, Frédérick. « L'art de la guerre revisité. Cyberstratégie et cybermenace chinoises », *La Découverte*, n°152-153, 2014, p.161-173. [file:///C:/Users/F%C3%A9lix/Downloads/HER_152_0161.pdf]

DW. « Germany launches cybersecurity agency to strengthen 'digital sovereignty' », *DW*, [En ligne], Le 8 novembre, 2020, [https://www.dw.com/en/germany-launches-cybersecurity-agency-to-strengthen-digital-sovereignty/a-54529134#:~:text=The%20German%20government%20has%20signed,cyberthreats%20to%20the%20country's%20security] (page consultée le 1 février 2021)

EMMOTT, Robin. « NATO cyber command to be fully operational in 2023 », *Reuters*, [En ligne], Le 16 octobre 2018, [NATO cyber command to be fully operational in 2023 | Reuters] (page consultée le 2 janvier 2021)

ESCHAPASSE, Baudouin. « Nouvelle cyberattaque contre des géants pétroliers », *LePoint*, [En ligne], Le 17 décembre 2017, [https://www.lepoint.fr/high-tech-internet/l-arabie-saoudite-sous-le-feu-de-hackers-25-01-2017-2099955_47.php] (page consultée le 29 janvier 2021)

FINLAY, Lorraine, et PAYNE, Christian. « Why international law is failing to keep pace with technology in preventing cyber attacks », *The Conversation*, [En ligne], Le 19 février 2019, [https://theconversation.com/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks-111998] (page consultée le 2 mars 2021)

FRANCE24. « Les États-Unis accusent la Russie d'une cyberattaque "majeure", Moscou dément », *France24*, [En ligne], Le 19 décembre 2020, [https://www.france24.com/fr/am%C3%A9riques/20201219-les-%C3%A9tats-unis-accusent-la-russie-d-une-cyberattaque-majeure-moscou-d%C3%A9ment] (page consultée le 2 janvier 2021)

FYFFE, Greg. « Should the Five Eyes Alliance be Expanded? », *Centre for International Policy Studies*, [En ligne], Le 19 octobre 2020, [https://www.cips-cepi.ca/2020/10/19/should-the-five-eyes-alliance-be-expanded/] (page consultée le 2 février 2021)

GAZULA B., Mohan. « Cyber Warfare Conflict Analysis and Case Studies », *Massachusetts Institute of Technology*, 2017, 99 pages. [https://web.mit.edu/smadnick/www/wp/2017-10.pdf] (page consultée le 22 décembre 2020)

GOCEK, Naz. « Brexit's Impact on NATO and European Security », *Association Canadienne pour l'OTAN*, [En ligne], Le 8 avril 2019, [https://natoassociation.ca/brexits-impact-on-nato-and-european-security/] (page consultée le 16 janvier 2021)

GORMAN, Siobhan, et COLE, August, et DREAZEN, Yochi. « Computer Spies Breach Fighter-Jet Project », *The Wall Street Journal*, [En ligne], Le 21 avril 2009, [https://www.wsj.com/articles/SB124027491029837401] (page consultée le 19 janvier 2021)

HANNA, Jason. « What is the Five Eyes intelligence pact? », *CNN*, [En ligne], Le 26 mai 2017, [https://www.cnn.com/2017/05/25/world/uk-us-five-eyes-intelligence-explainer/index.html] (page consultée le 13 janvier 2021)

HARRIS, Kathleen. « Liberals to create 'super' national security watchdog as part of anti-terror law overhaul », *CBC News*, [En ligne], Le 20 juin 2017, [https://www.cbc.ca/news/politics/security-terrorism-legislation-1.4168780] (page consultée le 19 janvier 2021)

HEMMING LAHMANN, Christian. « Unilateral remedies to cyber operations: self-defence, countermeasures, necessity, and the question of attribution », *Cambridge University Press*, 2020, 326 pages. [https://books-scholarsportal-info.proxy.bib.uottawa.ca/en/read?id=/ebooks/ebooks6/cambridgeonline6/2020-09-08/1/9781108807050#page=18] (page consultée le 19 décembre 2020)

HM GOVERNMENT. « National Cyber Security Strategy 2016-2021 », *HM Government*, [En ligne], [National Cyber Security Strategy 2016-2021 (publishing.service.gov.uk)] (page consultée le 15 janvier 2021)

HONGJU KOH, Harold. « International Law in Cyberspace », *Havard International Law Journal*, Vol. 54, 2012, 12 pages. [International Law in Cyberspace (yale.edu)] (page consultée le 17 décembre 2020)

HOSMER T., Stephen. « The Conflict Over Kosovo: Why Milosevic Decided to Settle When He Did », *RAND Corporation*, 2001, p. 65-76. [https://www.jstor.org/stable/10.7249/mr1351af.13] (page consultée le 18 décembre 2020)

IBM. « What is a cyber attack », *IBM*, [En ligne], Le 1 décembre 2020, [https://www.ibm.com/services/business-continuity/cyber-attack], (page consultée le 4 mars 2021)

INTERNATIONAL TELECOMMUNICATIONS UNION. « Statistics », *International Telecommunications Union*, [En ligne], Mise à jour le 18 janvier 2021,

[https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx] (page consultée le 25 janvier 2021)

JABBARI, Cyrus. « The Application of International Law in Cyberspace: State of Play », *Office of Disarmament Affairs, United Nations*, [En ligne], 25 octobre 2018, [https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/] (page consultée le 5 janvier 2021)

JANCZEWSKI, Robert, et PILARSKI, Grzegorz, et MARCZYK, Maciej. « Terminology as a Barrier to NATO's Interoperability in Cyberspace Operations », *International Conference Knowledge-Based Organization*, Vol. 25, nº 3, 2019, p.31-35. DOI: https://doi.org/10.2478/kbo-2019-0113

JI YOUNG, Kong, et JONG IN, Lim, et KYOUNG GON, Kim. « The All-Purpose Sword: North Korea's Cyber Operations and Strategies », *NATO CCDCOE Publications*, 2019, 20 pages. [CyCon_2019_Kong_Kim_Lim.indd (ccdcoe.org)] (page consultée le 5 février 2021)

LAWSON, Sean. « Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats », *Journal of information Technology and Politics*, Vol. 10, 2013, p.86-103. [C:\iTools\WMS\TandF-Journals\3833133\WorkingFolder\WITP_A_759059.dvi (uottawa.ca)] (page consultée le 22 décembre 2020)

LEMAÎTRE, Frédéric. « La Chine, bulldozer de la croissance mondiale », *LeMonde*, [En ligne], Le 12 janvier 2021, [https://www.lemonde.fr/economie/article/2021/01/12/la-chine-bulldozer-de-la-croissance-mondiale_6065927_3234.html] (page consultée le 11 janvier 2021)

LE MONDE. « L'OTAN ouvre une enquête sur l'incident entre la France et la Turquie en Méditerranée », *LeMonde*, [En ligne], Le 18 juin 2020, [https://www.lemonde.fr/international/article/2020/06/17/paris-denonce-une-man-uvre-turque-recente-extremement-agressive-en-mediterranee_6043175_3210.html] (page consultée 19 décembre 2020)

LÉTÉ, Bruno, et DEGE, Daiga. « NATO Cybersecurity: A Roadmap to Resilience », *The German Marshall Fund of the United States*, Vol. 23, 2017, 6 pages. [https://www.jstor.org/stable/resrep18857] (page consultée le 7 février 2021)

LEWIS ANDREW, James. « Economic Impact of Cybercrime », *Center for Strategic and International Studies*, [En ligne], le 21 février 2018, [Economic Impact of Cybercrime | Center for Strategic and International Studies (csis.org)] (page consultée le 12 janvier 2020)

LEWIS, Don. « What is NATO Really Doing in Cyberspace? », *War On the Rocks*, [En ligne], Le 4 février 2019, [What Is NATO Really Doing in Cyberspace? - War on the Rocks] (page consultée le 3 février 2021)

LILLY, Bilyana, CHERAVITCH, Joe. « The Past, Present, and Future of Russia's Cyber Strategy and Forces », *RAND Corporation*, 2020, p.129-155. [CyCon_2020_book.indd (ccdcoe.org)] (page consultée le 29 janvier 2021)

LOHARD, Audrey. « La genèse inattendue du cyberespace de William Gibson », *Persée*, no.66, 2008, p.11-13. [https://www.persee.fr/doc/quad_0987-1381_2008_num_66_1_1842] (page consultée le 10 septembre 2020)

LONSDALE J., David. « Warfighting for Cyber Deterrence: a Strategic and Moral Imperative », *Philosophy and Technology*, Vol.31, nº 3, Septembre 2018, p.409-429. [http://dx.doi.org.proxy.bib.uottawa.ca/10.1007/s13347-017-0252-8]

LUCAS, George. « Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare », *Oxford University Press*, 2017, 256 pages. [Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of ... - George Lucas - Google Livres] (page consultée le 10 octobre 2020)

LUXNER, Larry. « Will NATO still be relevant in the future? », *Atlantic Council*, [En ligne], Le 24 juillet 2020, [Will NATO still be relevant in the future? - Atlantic Council] (page consultée le 20 décembre 2020)

MARMOUYET, Françoise. « Les pays de l'Otan face à l'isolationnisme version Donald Trump », *France24*, [En ligne], Le 13 novembre 2016, [https://www.france24.com/fr/20161111-donald-trump-otan-budget-europe-securite] (page consultée 5 janvier 2021)

MINISTÈRE DES ARMÉES. « Communiqué_La France se dote d'une doctrine militaire offensive dans le cyberespace et renforce sa politique de lutte informatique défensive. », *Ministère des armées*, [En ligne], Le 18 janvier 2019, [Communiqué_La France se dote d'une doctrine militaire offensive dans le cyberespace et renforce sa politique de lutte informatique défensive. (defense.gouv.fr)] (page consultée le 23 janvier 2021)

MOYNIHAN, Harriet. « The Application of International Law to State Cyberattacks, Sovereignty and Non-intervention », *The Royal Institute of International Affairs*, 2019, 60 pages. [https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf] (page consultée le 18 janvier 2021)

MURRAY, Rob. « L'Alliance a tout intérêt à se doter d'une filière d'innovation résiliente », *NATO Review*, [En ligne], Le 1 septembre 2020, [L'Alliance a tout intérêt à se doter d'une filière d'innovation résiliente (nato.int)] (page consultée le 8 mars 2021)

NATIONS UNIES. « Projet d'articles sur la responsabilité de l'État pour fait international illicite », *Nations Unies*, [En ligne], 2001, p.388-404. [https://legal.un.org/ilc/texts/instruments/french/draft_articles/9_6_2001.pdf]

NATIONS UNIES. « Conflit et violence : une ère nouvelle », *Nations Unies*, [En ligne], [https://www.un.org/fr/un75/new-era-conflict-and-violence] (page consultée le 28 décembre 2020)

NATIONS UNIES. « La Charte des Nations Unies : Chapitre I », Nations Unies, 1945, [Chapitre I | Nations Unies]

NATOCCDCOE. *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, [Vidéo en ligne], Le 9 juillet 2019, [NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) - YouTube] (vidéo consultée le 19 janvier 2021)

NATO COMMUNICATIONS AND INFORMATION AGENCY. « Three NATO Industry Cyber Partnership agreements signed at NIAS'19 », *NATO Communications and Information Agency*, [En ligne], Le 17 octobre 2019, [NCI Agency | Three NATO Industry Cyber Partnership agreements signed at NIAS'19] (page consultée le 1 février 2021)

NOCETTI, Julien. « Géopolitique de la cyber-conflictualité », *Politique étrangère*, Vol. 2, 2018, p.15-27. DOI : 10.3917/pe.182.0015. [https://www-cairn-info.proxy.bib.uottawa.ca/revue-politique-etrangere-2018-2-page-15.htm]

NORTH ATLANTIC TREATY ORGANIZATION. « NATO Cyber Defense », *North Atlantic Treaty Organization*, [En ligne], 2016. [https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf] (page consultée le 29 décembre 2020)

NORTH ATLANTIC TREATY ORGANIZATION. « NATO Leaders: Lord Ismay », *North Atlantic Treaty Organization*, [https://www.nato.int/cps/us/natohq/declassified_137930.htm] (page consultée le 3 janvier 2021)

N. SCHMITT, Michael, et collab. « Tallinn Manuel on the International Law Applicable to Cyber Warfare », *Cambridge University Press*, New York, 2013, 282 p. [356296245.pdf (peacepalacelibrary.nl)]

NURKULOV, Nurshod. « New Cyber Strategy of China and the Altercation in the Field », *Journal of Political Science and Public Affairs*, Vol. 5, nº 4, Le 6 novembre 2017, 6 pages. DOI: 10.4172/2332-0761.1000307

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. « Fiche terminologique », Office québécois de la langue française, [En ligne], [http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8351162] (page consultée le 24 janvier 2021)

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD. « Le Traité de l'Atlantique Nord », *Organisation du traité de l'Atlantique nord*, [En ligne], Le 4 avril 1949, [NATO - Official text: Le Traité de l'Atlantique Nord, 04-Apr.-1949] (page consultée le 22 janvier 2021)

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD. « L'OTAN se défendra », *Organisation du traité de l'Atlantique nord*, [En ligne], Le 27 août 2019, [NATO - News: NATO will defend itself (Article by NATO Secretary General Jens Stoltenberg published in Prospect), 27-Aug.-2019] (page consultée le 29 janvier 2021)

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD. « Cyberdéfense », *Organisation du traité de l'Atlantique nord*, [En ligne], Mise à jour le 20 octobre 2020, [https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=fr] (page consutlée le 19 décembre 2020)

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD. « Remarks », *Organisation du traité de l'Atlantique nord*, [En ligne], Le 23 mai 2019, [NATO - Opinion: Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London, 23-May.-2019] (page consultée le 15 janvier 2021)

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD. « Déclaration du sommet du Pays de Galles », *Organisation du traité de l'Atlantique nord*, [En ligne], Le 5 septembre 2014. [NATO - Official text: Déclaration du sommet du Pays de Galles publiée par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue au pays de Galles, 05-Sep.-2014] (page consultée le 22 janvier 2021)

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD. « Approche de l'OTAN concernant l'espace », *Organisation du traité de l'Atlantique nord*, [En ligne], Le 27 octobre 2020, [NATO - Topic: NATO's approach to space] (page consultée le 17 décembre 2020)

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD. « Cyberdéfence », *Organisation du traité de l'Atlantique nord*, [En ligne], Le 20 octobre 2020, [NATO - Cyber defence] (page consultée le 3 janvier 2021)

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD. « Engagement en faveur de la cyberdéfense », *Organisation du traité de l'Atlantique nord*, [En ligne], Le 8 juillet 2016, [NATO - Official text: Cyber Defence Pledge, 08-Jul.-2016] (page consultée le 3 février 2021)

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD. « Défense intelligente », *Organisation du traité de l'Atlantique nord*, [En ligne], Le 30 mars 2017, [NATO - Topic: Smart Defence] (page consultée le 2 février 2021)

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD. « Relations avec l'Union européenne », *Organisation du traité de l'Atlantique nord*, [En ligne], Le 31 juillet 2020, [https://www.nato.int/cps/fr/natohq/topics_49217.htm] (page consultée le 1 février 2021)

OTTIS, Rain. « Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective », *Cooperative Cyber Defence Centre of Excellence*, 2008, [https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf]

PANAGIOTIS EFTHYMIOPOULOS, Marios. « A cyber-security framework for development, defense and innovation at NATO », *Journal of Innovation and Entrepreneurship*, Vol. 8, n° 1, 2019, 26 pages. DOI: 10.1186/s13731-019-0105-z

PAUL, Kari, et BECKETT, Lois. « What we know – and still don't – about the worst-ever US government cyber-attack », *The Guardian*, [En ligne], 19 décembre 2020, [https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government] (page consultée le 19 décembre 2020)

PRUNKUN, Henry. « Cyber Weaponry », *Springer International Publishing*, Sydney, 2018, 198 p. [https://doi.org/10.1007/978-3-319-74107-9]

RADIO-CANADA. « Une cyberattaque chinoise stoppée avant que 900 000 entreprises en soient victimes », *Radio-Canada*, [En ligne], Le 7 février 2019, [https://ici.radio-canada.ca/nouvelle/1151627/chine-piratage-apt10-visma-attaque-infonuagique] (page consultée le 3 janvier 2020)

RAUD, Mikk. « China and Cyber: Attitudes, Strategies, Organisation », *NATO Cooperative Cyber Defence Centre of Excellence*, 2016, 34 pages. [https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf]

RILEY, Tonya. « The Cybersecurity 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds », *The Washington Post*, [En ligne], Le 7 décembre 2020, [The Washington Post: Breaking News, World, US, DC News and Analysis] (Page consultée le 20 décembre 2020)

ROBERTSON, Tom, et VAN HOEVE, Simon. « Offensive Shifts, Offensive Policies: Cybersecurity Trends in the Government-Private Sector Relationship », *Canadian Global Affairs Institut*, [En ligne], 2019, [Offensive Shifts, Offensive Policies: Cybersecurity Trends in the Government-Private Sector Relationship - Canadian Global Affairs Institute (cgai.ca)] (page consultée le 11 janvier 2021)

SCHALLBRUCH, Martin, et MARIE SKIERKA, Isabel. « The Evolution of the German Cybersecurity Strategy », *Springer Briefs in Cybersecurity*, 2018, 14 pages. DOI: 10.1007/978-3-319-90014-8_3

SÉCURITÉ PUBLIQUE CANADA. « Stratégie nationale de cybersécurité », *Sécurité publique Canada, Gouvernement du Canada*, [En ligne], mise à jour le 28 mai 2019. [https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx] (page consultée le 21 janvier 2021)

SHAKARIAN, Paulo. « The 2008 Russian Cyber Campaign Against Georgia », *Military Review*, 2011, p.63-69. [file:///C:/Users/F%C3%A9lix/Downloads/SHAKARIAN-RussiaCyber-MilRev.pdf] (page consultée le 1 janvier 2021)

SOLENDER, Andrew. «'I Will Not Stand Idly By': Biden Says Cybersecurity Will Be 'Top Priority' After Giant Hack », *Forbes*, [En ligne], Le 17 décembre 2020, [https://www.forbes.com/sites/andrewsolender/2020/12/17/i-will-not-stand-idly-by-biden-says-cybersecurity-will-be-top-priority-after-giant-hack/?sh=412ac4705159] (page consultée le 10 janvier 2021)

SPILLMANN, Christian. « L'OTAN classe les années Trump et attend Joe Biden », *LaPresse*, [En ligne], Le 1 décembre 2020, [https://www.lapresse.ca/international/europe/2020-12-01/l-otan-classe-les-annees-trump-et-attend-joe-biden.php] (page consultée le 6 janvier 2021)

STEWART, Heather. « Mike Pompeo praises UK decision to remove Huawei from 5G network », *The Guardian*, [En ligne], Le 21 juillet 2020, [https://www.theguardian.com/us-news/2020/jul/21/mike-pompeo-praises-uk-decision-to-remove-huawei-from-5g-network] (Page consultée le 12 janvier 2021)

THE ECONOMIST. « A new global ranking of cyber-power throws up some surprises », *The Economist*, [En ligne], Le 17 septembre, 2020, [https://www.economist.com/science-and-technology/2020/09/17/a-new-global-ranking-of-cyber-power-throws-up-some-surprises] (Page consultée le 11 janvier 2021)

THE FEDERAL GOVERNMENT. « 2016 White Paper on German Security Policy and the Future of the Bundeswehr », *The Federal Government*, [En ligne], 2016. [2016-White-Paper-1.pdf (ccdcoe.org)] (page consultée le 17 janvier 2021)

THORNTON, Rod, MIRON, Marina, « Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom », *Journal of Cyber Policy*, Vol. 4, n° 2, 2019, p.257-274. [https://journals-scholarsportal-info.proxy.bib.uottawa.ca/pdf/23738871/v04i0002/257_drcwtpcfbtuk.xml] (page consultée le 3 décembre 2020)

TUCKER, Patrick. « NATO Getting More Aggressive on Offensive Cyber », *Defense One*, [En ligne], Le 24 mai 2019, [NATO Getting More Aggressive on Offensive Cyber - Defense One] (page consultée le 21 décembre 2020)

UNION INTERPARLEMENTAIRE ET COMITÉ INTERNATIONAL DE LA CROIX-ROUGE. « Droit international humanitaire », *Union interparlementaire et Comité international de la Croix-Rouge*, [En ligne], 2016, 138 p. [http://archive.ipu.org/PDF/publications/ihl-fr.pdf] (page consultée le 2 mars 2021)

UNITED NATIONS GENERAL ASSEMBLY. « Open-ended working group on developments in the field of information and telecommunications in the context of international security (A/AC.290/2021/CRP.2) », *United Nations*, [En ligne], Le 10 mars 2021, [file:///C:/Users/F%C3%A9lix/Downloads/Final-report-A-AC.290-2021-CRP.2.pdf] (page consultée le 14 mars 2021)

UNITED STATES OF AMERICA DEPARTMENT OF DEFENSE. « 2018 Department of Defense Cyber Strategy », *Department of Defense*, [En ligne], 2018, [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF] (page consultée le 2 février 2021)

VANDAL, Gilles. « Une remise en question des alliances comme l'OTAN », *La Tribune numérique*, [En ligne], Le 12 août 2018, [https://www.latribune.ca/opinions/une-remise-en-question-des-alliances-comme-lotan-d808fa74d45d5112500771a43c54aa4f] (page consultée le 5 janvier 2021)

VITKINE, Benoît. « L'Estonie, première cybervictime de Moscou », *LeMonde*, [En ligne], Le 14 mars 2017, [https://www.lemonde.fr/international/article/2017/03/14/l-estonie-premiere-cybervictime-de-moscou_5093948_3210.html] (page consultée le 2 janvier 2021)

ZECCHINI, Laurent, et TRUC, Olivier. « Les cyberattaques massives d'origine russe contre l'Estonie préoccupent l'Alliance atlantique », *LeMonde*, [En ligne], Le 26 mai 2008, [https://www.lemonde.fr/europe/article/2007/05/19/les-cyberattaques-massives-d-origine-russe-contre-l-estonie-preoccupent-l-alliance-atlantique_912244_3214.html] (page consultée le 21 décembre 2020)