Institut Royal Supérieur de Défense

LA DÉFENSE

SÉCURITÉ & STRATÉGIE N°139
Février 2019

L'implication de la Belgique dans la cyberstratégie euro-atlantique : état des lieux et défis à relever

Estelle Hoorickx

Février 2019

L'implication de la Belgique dans la cyberstratégie euro-atlantique : état des lieux et défis à relever

Estelle Hoorickx

Institut Royal Supérieur de Défense
Centre d'Etudes de Sécurité et Défense
30 Avenue de la Renaissance
1000 Bruxelles

ISSN 2295-0915

Une version électronique du présent document est disponible et peut être téléchargée gratuitement sur notre site internet : www.irsd.be.

Vos questions, remarques ou commentaires relatifs au présent document peuvent être adressés au :
Directeur du Centre d'Etudes de Sécurité et Défense
Institut Royal Supérieur de Défense
30 Avenue de la Renaissance
1000 Bruxelles
ou par courriel à : +IRSD-CESD-SCVD@mil.be

L’auteure

Le Cdt d’Avi Estelle Hoorickx est attachée de recherche au Centre d’Études de Sécurité et Défense de l’Institut Royal Supérieur de Défense (IRSD). Ses domaines de compétence englobent les développements conceptuels dans l’emploi des capacités de Défense, les menaces hybrides, la cybersécurité, le terrorisme en Europe et le rôle de la Belgique dans les organisations internationales. Elle effectue un doctorat en histoire sur l’influence de ce pays à l’OTAN pendant la Guerre froide.

Executive Summary

Cyberattacks are now amongst the highest-likelihood risks in the world, along with natural disasters, large-scale migration movements, inter-state conflicts and terrorist attacks. The potential danger of cyber threats has been known to the EU and NATO ever since the early 2000s, but drawing up a Euro-Atlantic defence cyberstrategy has been for them a relatively recent concern. The development and increased complexity of computer hacking with major military consequences has affected how the EU and NATO are considering cyberspace protection, paving the way for new strategies. To prevent and respond to cyberattacks in a crisis management context, both institutions have recently decided to share a number of information data related to cyber defence in order to avoid redundant activities and capabilities. The crucial challenge Euro-Atlantic defence cyberstrategy is facing is the determining role states can play in protecting information systems and providing potential strategic responses to cyberattacks.

Assessing a nation's ability to take action in cyberspace differs according to the chosen criteria and remains a difficult process. Belgium, which is comparatively mature in terms of cybersecurity, has been actively contributing to the Euro-Atlantic defence cyberstrategy. The current challenge for Belgian authorities is to adjust the existing legal, organizational and technical means for an appropriate response to cyber threats. This study is in two parts. The first part discusses the impact of increasingly complex hacking events on the implementation of a Euro-Atlantic defence cyberstrategy, with special emphasis on national responsibilities for securing cyberspace stability. The second part studies Belgium's cyberstrategy and the major challenges it faces in order to meet its Euro-Atlantic cybersecurity and cyber defence obligations.

Les cyberattaques font partie, depuis quelques années, des risques dont la probabilité de survenance est la plus élevée à travers le monde, au même titre que les catastrophes naturelles, les mouvements de migration à grande échelle, les conflits interétatiques ou les attaques terroristes. Si la prise de conscience du danger cybernétique par l'UE et l'OTAN remonte au début des années 2000, la mise en place d'une cyberstratégie euro-atlantique en matière de défense est relativement récente. Le développement et la complexification des piratages informatiques aux retombées militaires à grande échelle rend la mission de protection du cyberespace par ces deux organisations plus difficile et ouvre la voie à de nouvelles stratégies. Pour prévenir et faire face aux cyberattaques dans un contexte de gestion de crise, les deux organisations ont depuis peu décidé de mettre en commun un certain nombre d'informations liées à la cyberdéfense, ce qui permet d'éviter la redondance des activités et capacités. La cyberstratégie euro-atlantique se heurte néanmoins à un enjeu crucial: le rôle déterminant des États dans la protection des systèmes d'information et dans la réponse stratégique à apporter en cas de cyberattaque d'un pays allié.

Évaluer la capacité d'un État à agir dans le cyberespace diffère selon les critères choisis et reste difficile. La Belgique, pays relativement mature en matière de cybersécurité, contribue activement à la stratégie euro-atlantique. Le défi actuel des autorités belges consiste à ajuster les moyens juridiques, organisationnels et techniques existants afin de disposer d'une réponse appropriée face aux cybermenaces. La présente étude comporte deux parties. La première a pour but de discerner l'impact du développement et de la complexification des piratages informatiques sur la mise en place d'une cyberstratégie euro-atlantique. Il s'agira également de déterminer le rôle joué par les États dans la stabilité du cyberespace. La seconde partie analyse

la cyberstratégie de la Belgique et les défis à relever par ce pays pour remplir ses obligations euro-atlantiques en matière de cybersécurité et de cyberdéfense.

Table des matières

Liste des abréviations et acronymes

ACOS IS	Assistant Chief of Staff Intelligence and Security (département d'état-major Renseignement et Sécurité)
ACOS O&T	Assistant Chief of Staff Operations and Training (département d'état-major Opérations et Entraînement)
BSA	Business Software Alliance
CCB	Centre pour la cybersécurité Belgique
CERT	Computer Emergency and Reponse Team
CSIRT	Computer Security Incident Respone Team
DGA	Direction générale de l'armement
ERM	École Royale Militaire
FCCU	Federal Computer Crime Unit
FEB	Fédération des Entreprises de Belgique
GAFAM	Google, Amazon, facebook, Apple et Microsoft
GPS	Global Positioning System
HM Government	Her Majesty's Government (UK Government)
IA	Intelligence artificielle
IBPT	Institut belge des services postaux et des télécommunications
ICT	Information and Communication Technology
IDE	Investissements directs à l'étranger
IoT	Internet of Things (Internet des Objets)
IP	Internet protocol
IRSD	Institut Royal Supérieur de Défense
ITU	International Telecommunication Union
LBDSN	Livre blanc sur la Défense et la Sécurité nationale
LPM	Loi de programmation militaire
MGI	McKinsey Global Institute
MoU	Memorandum of Understanding
NDA	National Distribution Agency
NICP	Nato Industry Cyber Partnership
NIS	Network and Information Security
NSA	National Security Agency
OIV	Opérateurs d'importance vitale
PIB	Produit intérieur brut
RGPD	Règlement Général sur la Protection des Données
SGRS	Service de renseignement et de sécurité des forces armées.
SPF	Service public fédéral
SRI	Sécurité des réseaux et des systèmes d'information
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TIC	Technologies de l'information et de la communication
UE	Union européenne
UIT	Union internationale des télécommunications
UNGGE	UN Group of Governemental Experts
UP KRITIS	Umsetzungsplan Kritische Infrastructuren (plan de mise en oeuvre des infrastructures critiques)

Introduction

« *L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique* » disait Albert Einstein. Si la prise de conscience du danger cybernétique par l'UE et l'OTAN remonte au début des années 2000, la mise en place d'une cyberstratégie euro-atlantique en matière de défense est relativement récente.

Selon l'accord du gouvernement belge du 9 octobre 2014, «*Considérant les dangers auxquels sont confrontés nos institutions, nos entreprises et nos citoyens, la cybersécurité constituera une priorité*»[1]. Par ailleurs, un des objectifs de « la vision stratégique pour la Défense belge » de 2016 est que celle-ci soit en mesure d'apporter une réponse adéquate aux menaces cyber en développant une « *capacité cybernétique propre, composée d'un pilier défensif, offensif et du renseignement* »[2]. La nouvelle cyberstratégie, qui sera publiée en 2019, envisagera l'intégration du cyberespace comme nouveau domaine opérationnel.

L'objectif de la présente étude consiste à analyser la cyberstratégie développée par la Belgique afin de garantir sa cybersécurité et participer au projet euro-atlantique. De cette problématique principale découlent d'autres questions auxquelles il s'agira de répondre: quels sont les défis et menaces cybernétiques auxquels l'UE et l'OTAN sont confrontés ? Quelles sont les cyberstratégies menées par ces deux organisations ? Quelles sont les actions spécifiques menées par les États pour traiter des problèmes de sécurité dans le cyberespace euro-atlantique ? Quel est le degré de maturité des États, et singulièrement de la Belgique, en matière de cybersécurité ?

Pour répondre à ces différentes questions, l'étude comporte deux parties. La première a pour but de discerner le développement et la complexification des piratages informatiques ainsi que leur impact sur la mise en place d'une cyberstratégie euro-atlantique. Si les deux organisations ont des priorités stratégiques spécifiques, elles désirent, depuis peu, coopérer en matière de cyberdéfense. Par ailleurs, les États et les compagnies privées jouent un rôle majeur dans la mise en œuvre de la cyberstratégie euro-atlantique.

La seconde partie analyse la stratégie nationale belge en matière de cybersécurité et de cyberdéfense mais également les mesures prises par la Belgique pour participer à la stratégie euro-atlantique.

Pour terminer, la présente étude proposera un certain nombre de conclusions et recommandations sur l'environnement cybernétique actuel, la stratégie euro-atlantique, le rôle des États comme cyberpuissances et le degré de maturité de la Belgique en matière de cybersécurité.

---

[1] *Accord de gouvernement de la Belgique*, 9 octobre 2014, p. 148.

[2] *La Vision stratégique pour la défense*, 29 juin 2016, p. 100.

Partie 1 : Évolution de la cyberstratégie euro-atlantique et défis actuels[3]

La cyberinsécurité, un enjeu mondial crucial

Depuis les attaques informatiques massives qui ont frappé l'Estonie en 2007, il ne se passe pratiquement pas une semaine sans que l'on annonce, quelque part dans le monde, une cyberattaque importante. Ce terme générique désigne une agression informatique, pouvant faire référence à une technique d'attaque ou à un objectif de l'attaquant. Largement utilisé, il désigne en fait plusieurs types d'agressions de nature et aux conséquences très diverses comme le défacement[4], les attaques en déni de service[5] au moyen d'un logiciel malveillant, ou encore des attaques à but d'espionnage ou de sabotage[6]. Le préfixe cyber est dérivé de l'adjectif grec *κυβερνητικός* signifiant « doué pour le mouvement » ou, au sens figuré, « doué pour diriger, gouverner ». Le terme sera repris plus tard sous le vocable « cybernétique », dont l'usage sera largement diffusé à la suite de la publication, en 1948, de l'ouvrage de science-fiction *Cybernetics* par Norbert Wiener. Il se définit comme la « *science des théories sur les processus de commande et de communication et leur régulation chez l'être vivant, dans les machines et dans les systèmes sociologiques et économiques* » [7].

Le risque d'incident cyber est d'autant plus grand que le nombre d'internautes ne cesse d'augmenter. Alors qu'en 1995, moins d'1% de la population mondiale a accès à internet, ce chiffre s'élève à 7 % en 2000, 30 % en 2010[8] et 48,2% en 2018, soit un nombre actuel de 3,6 milliards d'internautes[9]. Si, au début des années 2000, la plupart des internautes viennent des États-Unis et d'Europe, ce n'est plus le cas aujourd'hui. Début 2017, le nombre d'internautes en Chine (739 millions) dépassait celui, combiné, des États-Unis et de l'Union européenne (718 millions)[10]. Ce sont en effet la

[3] La présente partie de l'étude a fait l'objet d'un article intitulé : « Une cyberstratégie euro-atlantique en matière de défense : mythe ou réalité ? », *Stratégique*, n°117, 2018 (E. Hoorickx).

[4] Les attaques de « *défacement* » ou « *défiguration* » de sites internet visent à en modifier l'apparence sans l'assentiment de leurs titulaires, pour signaler une faille de sécurité, nuire à la réputation de la marque ou du titulaire du site, ou tout simplement par provocation ou revendication (A. Desforges et E. Déterville, *Lexique sur le cyberespace*, *Hérodote*, n° 152-153, 2014/1, p. 24).

[5] Les « attaques en déni de service » (DOS-*Deny of Service*) sont destinées à interdire aux utilisateurs légitimes d'un service internet de l'utiliser, en perturbant son fonctionnement et pouvant conduire à son blocage (Ch. Aghroum, *Les mots pour comprendre la cybersécurité. Et profiter sereinement d'Internet*, Paris, 2010, p. 18).

[6] A. Desforges et E. Déterville, *op. cit.*, pp. 23-24.

[7] O. Kempf, *Introduction à la cyberstratégie*, Paris, 2012, p. 5.

[8] The World Bank Group, *Individuals using the Internet (% of population)*, 2017 (https://data.worldbank.org/indicator/IT.NET.USER.ZS, consulté le 17 décembre 2018).

[9] S.n., *eMarketer Updates Worldwide Internet and Mobile User Figures*, 6 décembre 2017 (https://www.emarketer.com).

[10] *ITU (International Telecommunication Union)-Key-2005-2017-ICT-data.xls*; J. Nocetti, « Internet et sa gouvernance : crispations internationales et nouveaux enjeux », dans S. Taillat, A. Cattaruzza et D. Danet, La Cyberdéfense. Politique de l'espace numérique, Paris, 2018, p. 131.

Chine et l'Inde, pays fortement peuplés, qui accueillent ensemble le plus grand nombre de personnes connectées, malgré une connectivité nationale globalement peu élevée[11].

Au total, en 2016, 80 % des entreprises européennes auraient été victimes d'une cyberattaque, et ce principalement par rançonlogiciel (4000 attaques quotidiennes recensées à travers le monde)[12]. Le rançonlogiciel ou *ransomware* est un type de logiciel malveillant qui bloque complètement ou partiellement l'accès des utilisateurs à leur système par un verrouillage de leur écran d'ordinateur ou de leurs fichiers, jusqu'à ce qu'une rançon soit payée[13].

En 2016, l'OTAN a traité en moyenne 500 incidents par mois, soit une augmentation d'environ 60% par rapport à 2015. Au cours de l'année 2017, les experts en cybersécurité de l'Alliance ont noté une évolution des cyberattaques et « *un ciblage croissant des systèmes les plus vulnérables, tels que les appareils personnels et les réseaux liés à l'OTAN mais non protégés par elle* »[14].

En mai 2017, l'attaque au moyen du logiciel rançonneur Wannacry touche près de 400 000 ordinateurs dans plus de 150 pays. Un mois plus tard, les rançonlogiciels Petya et NotPetya frappent l'Ukraine et plusieurs entreprises dans le monde entier[15]. Ces deux cyberattaques entraînent environ 300 millions de dollars de perte d'activité pour des entrerpises comme Merck (compagnie pharmaceutique allemande), FedEx et Maersk (compagnie maritime danoise)[16]. Plus récemment encore, le service de renseignement de l'armée russe (GRU-*Glavnoyé Razvédyvatel'noyé Oupravléniyé*), déjà accusé d'avoir interféré dans les élections américaines de 2016, a été mis sur la sellette en octobre 2018 par un certain nombre de pays occidentaux pour avoir lancé des cyberattaques tous azimuts sur de nombreuses organisations internationales. Parmi elles figurent l'Agence mondiale antidopage (AMA), le Comité olympique international (CIO), la Fédération internationale de football (FIFA) ou l'Organisation pour l'interdiction des armes chimiques (OIAC) à La Haye. Moscou dément ces accusations[17]. Depuis quelque temps enfin, le géant chinois des réseaux et de la téléphonie mobile Huawei, actif dans plus de 140 pays, est soupçonné de cyberespionnage un peu partout dans le monde, notamment en Belgique[18].

---

[11] En 2016, la Chine comptait environ 721 millions d'internautes, soit 52% de sa population (contre 8,5% en 2005), l'Inde 462 millions, soit 35% de sa population (contre 2,4% en 2005) et les États-Unis 286 millions, soit 88,5 % de sa population (contre 68% en 2005) (C. Linnhoff-Popien, R. Schneider, M. Zaddach, *Digital Marketplaces Unleashed*, 2018, Munich, p. 842; The World Bank Group, *Individuals using the Internet (% of population)*, 2017).

[12] R. Danesi et L. Harribey, *Rapport d'information fait au nom de la commission des affaires européennes sur la cybersécurité dans l'Union européenne*, n°458, avril 2018, p. 9 (http://www.senat.fr/rap/r17-458/r17-4581.pdf, consulté le 7 décembre 2018) ; Commission européenne, « Cybersécurité et libre circulation des données dans l'UE », Bruxelles, 19 septembre 2017 (https://ec.europa.eu/commission/news/cybersecurity-and-free-flow-non-personal-data-eu-2017-sep-19_fr, consulté le 12 décembre 2018).

[13] Communication conjointe au Parlement européen et au Conseil. *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017 [JOIN (2017) 450 final], p. 2.

[14] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_11/20171128_1711-factsheet-cyber-defence-fr.pdf, consulté le 2 janvier 2019.

[15] Communication conjointe au Parlement européen et au Conseil. *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017 [JOIN (2017) 450 final], p. 2.

[16] Ponemon Institute, *2017 Cost of Cybercrime Study. Insights on the Security Investments that make a difference*, p. 15 (https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf, consulté le 13 décembre 2018).

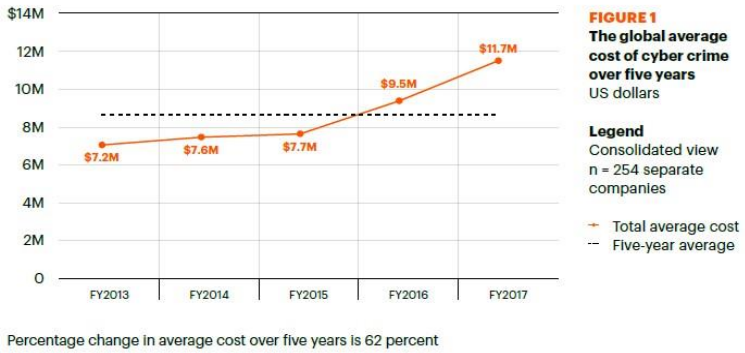
[17] Ch. Ly., « Les pays occidentaux dénoncent des cyberattaques sur plusieurs fronts de la part du renseignement russe (GRU) », dans *La Libre Belgique*, 5 octobre 2018, p. 17.

[18] S.n., « Huawei passée au crible par la Belgique», dans *l'Écho,* 7 décembre 2018, *L'Écho* https://www.lecho.be/tech-media/telecom/huawei-passee-au-crible-par-la-belgique/10076807.html, consulté le 14 décembre 2018)

Par ailleurs, selon *The New York Times*, le Conseil de l'Union européenne enquête activement sur le piratage, pendant plusieurs années, de milliers de câbles diplomatiques de l'UE. D'après « Area 1 », société spécialisée dans la cybersécurité, la technique déployée par les hackers sur une période de trois ans évoque celle d'une unité d'élite de l'armée chinoise[19].

Selon certaines études, l'incidence économique de la cybercriminalité aurait quintuplé entre 2013 et 2017, et pourrait encore quadrupler d'ici 2019 à travers le monde[20]. Une analyse publiée par l'entreprise de consultance Accenture et réalisée par l'institut Ponemon auprès de 254 entreprises issues de sept pays différents (Australie, France, Allemagne, Italie, Japon, Royaume-Uni et États-Unis) confirme cette constatation, de manière chiffrée cette fois. Á l'échelle mondiale, en 2017, le coût moyen du cybercrime aurait atteint 11,7 millions de dollars par entreprise, soit une augmentation de 23% par rapport à 2016. Le nombre médian des cyberattaques aurait également augmenté de 27,4% entre 2016 et 2017[21]. En outre, l'augmentation du coût de la cybercriminalité dans les entreprises étudiées serait, en moyenne, de 62 % entre 2013 et 2017[22] .

Augmentation du coût de la cybercriminaté entre 2013 et 2017[23]



Selon le *World Economic Forum*, les cyberattaques feraient partie depuis quelques années, des cinq risques dont la probabilité de survenance est la plus élevée à travers le monde, au même titre que les catastrophes naturelles, les mouvements de migration à grande échelle, les conflits interétatiques ou les attaques terroristes[24].

Enfin, les cyberattaques constitueraient, depuis 2018, le sixième risque dont l'impact économique est le plus important à l'échelle planétaire. Les répercussions financières que peuvent entraîner les catastrophes climatiques ou les mouvements migratoires, par exemple, inquiètent néanmoins davantage les scientifiques[25].

---

[19] D. E. Sanger et S. Erlanger, « Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran », dans The New York times, 18 décembre 2018 (https://www.nytimes.com/2018/12/18/us/politics/european-diplomats-cables-hacked.html, consulté le 16 janvier 2019).

[20] Communication conjointe au Parlement européen et au Conseil, *Résilience, op. cit.*.

[21] Ponemon Institute, *2017 Cost of Cybercrime Study*, *op. cit.*, pp. 2-3

[22] *Ibid.*, p. 12.

[23] *Ibid.*

[24] World Economic Forum, *The Global Risks Report 2018 13 th Edition*, 2018, p. 6 (http://www3.weforum.org/docs/WEF_GRR18_Report.pdf, consulté le 13 décembre 2018).

[25] *Ibid.*, pp. 3, 6.

C'est dans ce contexte particulièrement préoccupant que le thème du *Cyber Pearl Harbor* ou du « 9/11 numérique » [26] est apparu, il y a quelques années, dans la littérature académique. Nos sociétés savent en effet que leur dépendance aux réseaux interconnectés constitutifs de l'espace numérique peut leur être préjudiciable. D'aucuns craignent, outre les cyberattaques traditionnelles, l'apparition de nouveaux dangers cybernétiques comme l'attaque des infrastructures vitales par des terroristes ou même des criminels conventionnels ; la prolifération de cyber-armes très complexes qui deviendraient accessibles aux terroristes ; ou encore l'infiltration d'un virus, taillé sur mesure par une puissance étrangère, qui parviendrait à infiltrer une infrastrucutre structurelle, partagée, dans le pire des cas, par plusieurs banques, et qui en prendrait le contrôle[27].

Néanmoins, si les menaces et les attaques se multiplient et gagnent en sophistication, aucune catastrophe majeure, aucun effondrement ne s'est produit jusqu'ici. Comme le souligne Myriam Dunn Cavelty, « *il est [en effet] extrêmement improbable que les cyberacteurs avancés- comme les États-Unis, la Russie ou la Chine- lancent des cyberattaques sérieuses (de type Pearl Harbor) contre qui que ce soit en dehors d'un conflit militaire qui serait déjà en cours* »[28].

Depuis quelques années, il existe néanmoins, tant au sein de l'UE que de l'OTAN, une réelle volonté de mettre en place un cadre stratégique de cyberdéfense solide et cohérent. Si les deux organisations ont récemment reconnu le cyberespace comme nouveau domaine d'opérations[29], à l'instar des espaces terrestre, aérien et maritime[30], son utilisation comme zone de guerre, soit exclusivement, soit dans le cadre d'approches hybrides[31], est au cœur des débats[32].

Olivier Kempf définit le cyberespace comme « *l'espace constitué de systèmes informatiques de toute sorte connectés en réseaux et permettant la communication technique et sociale d'informations par des utilisateurs individuels ou collectifs* »[33]. Le cyberespace serait composé de trois couches : matérielle (constituée de tous les ordinateurs, systèmes informatiques et de l'infrastructure nécessaire à l'interconnexion), logique (tous les programmes informatiques qui traduisent l'information en données

---

[26] E. Bummiller, « Panetta Warns of Dire Threat of Xyberattack on US », New York Times, 11 octobre 2012; D. Charles, « US Homeland Chief: Cyber 9/11 Could Happen 'Imminetly'», Reuters, 24 janvier 2013 (articles cités par D. Danet, « Collapsologie numérique », *Stratégique*, n°117, 2018, p. 213.

[27] S.n., « La Cybersécurité : nous sommes tous concernés », [2017] (https://www.febelfin.be/fr/newsletter360/9/table-ronde-complete, consulté le 15 janvier 2019).

[28] M. Dunn Cavelty, « Un cyber Pearl Harbor : quelle probabilité à court terme ? », *Défense Sécurité Internationale*, numéro spécial, n°32, 2013, pp.30-32 (cité par D. Danet, *op. cit.*, p. 215).

[29] Le Centre d'excellence coopératif de cyberdéfénse de Tallinn définit le « cyberdomaine» comme un « espace de mise en relation de données numériques qui utilise le spectre électronique ou électromagnétique pour stocker, classer, traiter et transférer des données et des informations au travers de réseaux de télécommunications» (cité par G. Lasconjarias, « L'Otan et le domaine opérationnel cyber », dans S. Taillat, A. Cattaruzza et D. Danet, *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2018, p. 151)

[30] *Communiqué du Sommet de Varsovie publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Varsovie les 8 et 9 juillet 2016*, § 70 ; Communication conjointe au Parlement européen et au Conseil. *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017 [JOIN (2017) 450 final], p. 20.

[31] L'auteure analyse les pratiques de la « *guerre hybride* » dans l'étude: E. Hoorickx, « La défense contre les "menaces hybrides": la Belgique et la stratégie euro-atlantique », *Sécurité & Stratégie-IRSD*, n°131, octobre 2017.

[32] Communication conjointe au Parlement européen et au Conseil, *op. cit.*, p. 2.

[33] O. Kempf, *Introduction à la cyberstratégie*, Paris, 2012, p. 14.

numériques, qui utilisent cette information, et qui la transmettent) et enfin la couche sémantique, qui touche aussi bien l'activité des individus, mais aussi leurs interrelations, c'est-à-dire leur lien social[34].

Quels sont les défis et menaces cybernétiques auxquels l'UE et l'OTAN sont confrontés ? Existe-t-il une cyberstratégie euro-atlantique en matière de défense? Ces deux organisations sont-elles en mesure d'agir et de coopérer efficacement sur ce sujet? Quelles sont les actions spécifiques menées par les États pour traiter des problèmes de sécurité dans le cyberespace euro-atlantique ? Voilà quelques-unes des questions auxquelles la première partie de cette étude tentera d'apporter des éléments de réponse.

La cyberstratégie de l'UE et de l'OTAN : de quoi parle-t-on ?

Hew Strachan définit la stratégie comme « *une déclaration d'intention et un aperçu des moyens possibles pour mettre celle-ci en œuvre* »[35]. L'objectif de l'Alliance atlantique est clair : il s'agit de sauvegarder la paix et la sécurité des membres de l'OTAN par des moyens politiques et militaires, conformément aux principes de la Charte des Nations Unies. Pour mener à bien sa politique de sécurité, l'Alliance s'emploie à maintenir un potentiel militaire suffisant pour assurer une défense collective et une gestion des crises efficaces. La stratégie de l'UE nourrit, quant à elle, l'ambition de promouvoir les intérêts de ses citoyens en Europe mais également dans le monde[36]. Dès lors, « *la paix et la sécurité, la prospérité, la démocratie et un ordre mondial fondé sur des règles constituent les intérêts cruciaux qui sous-tendent [son] action extérieure*»[37]. Ceci suppose pour l'UE de renforcer sa « puissance civile » ou « puissance douce » (« *soft power* »)[38] mais également d'investir dans la sécurité et la défense, afin d' « *être crédible pour dialoguer de manière responsable avec le reste du monde* » [39], et singulièrement avec l'OTAN.

La cyberstratégie, serait, selon les termes d'Olivier Kempf, « *la branche de la stratégie propre au cyberespace*»[40]. Afin de réaliser au mieux leurs missions respectives, l'UE et l'OTAN ont un objectif stratégique clair. Il s'agit d'appliquer des mesures de sécurité afin de protéger leurs technologies ou systèmes d'information et de communication (TIC et SIC[41]) exposés aux cybermenaces[42]. Les

---

[34] *Ibid.*, pp. 10-13.

[35] H. Strachan, « Strategy and Contingency », *International Affairs*, vol. 87, n°6, novembre 2011, p. 1281.

[36] Note du Secrétariat général du Conseil de l'Union européenne intitulée « *Une stratégie globale pour la politique étrangère et de sécurité de l'Union européenne* », 28 juin 2016 [10715/16], pp. 4, 11.

[37] *Ibid.*, p. 11.

[38] *Ibid.*, p. 3.

[39] *Ibid.*, p. 39.

[40] O. Kempf, *Introduction à la cyberstratégie*, Paris, 2012, p. 25.

[41] L'UE utilise l'abréviation TIC pour désigner les « *Technologies de l'information et de la communication* » (*Information and Communication Technology-ICT*) là où l'OTAN préfère parler de SIC ou « *Systèmes d'information et de communication* » (*Communications and Informations Systems-CIS*).

[42] Pour expliquer le terme de « c*ybermenace* », un récent document du Parlement européen et du Conseil propose la définition suivante : « *toute circonstance ou tout événement potentiels susceptibles de porter atteinte aux réseaux et systèmes d'information, à leurs utilisateurs et aux personnes exposées* » (*Proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n°526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité), [COM(2017) 477 final]*, Bruxelles, 4 octobre 2017, p. 40).

extensions nationales des TIC/SIC ainsi que les systèmes qui remplissent des fonctions essentielles au sein des États, tels que les systèmes destinés aux pouvoirs publics, aux infrastructures critiques, à la sécurité et à la défense, peuvent également revêtir une importance cruciale pour l'UE et l'OTAN en cas de cyberattaque à l'échelle de tout un pays. Dès lors, si la cyberdéfense demeure une compétence clé des États, les cyberstratégies de ces deux organisations proposent aux pays membres des actions spécifiques qui permettent d'améliorer les performances globales de l'UE et de l'OTAN[43].

L'UE a tendance à qualifier la cyberstratégie de « cybersécurité »[44], là où l'OTAN privilégie le terme de « cyberdéfense »[45]. D'aucuns considèrent que ces deux termes sont interchangeables, alors qu'ils ont probablement des significations différentes[46]. Selon J.-M. Bockel, la cyberdéfense est une notion complémentaire de la cybersécurité, qui englobe la protection des systèmes d'information, la lutte contre la cybercriminalité[47] et la cyberdéfense[48]. Les efforts de cybersécurité dans l'UE auraient dès lors également une dimension de cyberdéfense[49]. L'Union veille en effet, depuis quelques années, à soutenir le développement des capacités de cyberdéfense de ses États membres, mises à disposition pour les missions et opérations de la politique de sécurité et de défense commune (PSDC)[50].

L'Alliance atlantique reste l'instance internationale la plus importante en matière de défense collective. Néanmoins, au vu de l'interpénétration des domaines de la cyberdéfense et de la cybersécurité ainsi qu'au caractère à double usage (civil et militaire) des cyberoutils et des cybertechnologies[51], il existe actuellement une volonté politique de la part de l'UE et de l'OTAN de coopérer davantage dans le domaine de la cyberdéfense.

L'UE et l'OTAN ont toujours veillé, depuis leur création, à sécuriser leurs systèmes de transmission respectifs. Depuis la fin des années 1990, le développement d'Internet à haut débit, et plus

---

[43] *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, février 2013, p. 5 ; *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2008/2004 (INI))*, § E et 5 ; *Communiqué du Sommet de Varsovie publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Varsovie les 8 et 9 juillet 2016*, § 71.

[44] La « cybersécurité » pourrait être définie comme « *toutes les activités nécessaires pour protéger les réseaux et les systèmes d'information, leurs utilisateurs et les personnes exposées contre les cybermenaces* » (*Ibid.*).

[45] L'OTAN définit la cyberdéfense comme « *the application of security measures to protect CIS infrastructure components against a cyber-attack* » (Colonel R. Ali, « *On Cyber Defence* », *The Three Swords Magazine*, n°26, 2014, p. 41). Selon le Parlement européen, « *la cyberdéfense intègre clairement des dimensions militaires et civiles* » (*Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense*, 2018, § A).

[46] Pour certains, la distinction entre cybersécurité et cyberdéfense serait triple : la sécurité serait l'affaire de la police et la défense serait le fait des armées ; la défense serait « *à l'extérieur* » (aux frontières ou en expéditionnaire) quand la sécurité serait à l'« *intérieur* » ; enfin, la sécurité serait un objectif à atteindre tandis que la défense serait le moyen d'y parvenir. Les stratégistes et spécialistes du sujet sont cependant loin de s'accorder sur la question (O. Kempf, *Introduction à la cyberstratégie*, Paris, 2012, pp. 52, 54).

[47] La convention de Budapest définit la cybercriminalité comme « l'ensemble des infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques » (A. Desforges et E. Déterville, *Lexique sur le cyberespace*, dans dans *Hérodote* 2014/1 (n°152-153), p. 23).

[48] J.-M. Bockel, *Rapport d'information du Sénat*, n°681, 18 juillet 2012, p. 10.

[49] Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, février 2013, p. 12.

[50] Conseil de l'Union européenne, *Cadre d'action de l'UE en matière de cyberdéfense [15585/14]*, Bruxelles, 18 novembre 2014, p. 4.

[51] Communication conjointe au Parlement européen et au Conseil. *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017 [JOIN (2017) 450 final], p. 20.

généralement du cyberespace, a bouleversé notre société. Notre quotidien, nos droits fondamentaux, notre vie sociale et notre économie dépendent désormais des technologies de l'information et des communications. Le développement et la complexification des piratages informatiques aux retombées militaires à grande échelle rend la mission de protection du cyberespace par l'UE et l'OTAN plus difficile et ouvre la voie à de nouvelles stratégies.

L'évolution de la cyberstratégie euro-atlantique face aux cyberattaques

Les cyberattaques de 2007 et 2008 : un « électrochoc pour la communauté internationale »[52]

Les premiers piratages informatiques à grande échelle remontent à la fin des années 1980. À l'époque, la démarche est essentiellement fondée sur la prouesse technologique[53]. Ce n'est qu'au début des années 2000 que les attaques cybernétiques commencent à viser, non plus seulement l'exploit pour lui-même, mais également des objectifs nettement mercantiles ou des buts militants, tels ceux défendus par le mouvement hacktiviste « *Anonymous* », qui utilise le piratage informatique dans le but de favoriser des changements politiques ou sociétaux[54]. L'Alliance atlantique prend conscience de l'importance de la cyberdéfense au début des années 2000, après avoir été victime de sa première cyberattaque lors de la guerre du Kosovo en 1999. Des activistes serbes, opposés aux bombardements de l'OTAN, attaquent alors la page Web du SHAPE par « défacement » et « déni de service »[55] . Si ces premiers cyberincidents[56] n'affectent pas directement la conduite des opérations militaires, ils conduisent à la prise de conscience de l'absence d'organisation centralisée pour l'ensemble des réseaux opérés par l'OTAN et de procédures de sécurité standardisées[57]. La problématique de cyberdéfense n'est cependant pas prise en compte dans le nouveau concept stratégique de l'Alliance, approuvé en avril 1999[58]. Il faut attendre le sommet de Prague de 2002 pour que les chefs d'État et de gouvernement de l'organisation préconisent de « *renforcer [les] capacités de défense [de l'Alliance] contre les*

---

[52] D. Ventre, « Les évolutions de la cybersécurité : contraintes, facteurs, variables… », *Étude Prospective et Stratégique*, n° 1506388759, juin 2015, p. 2.

[53] N. Arpagian, *La cybersécurité, Que sais-je ?*, 2010, p. 15.

[54] *Ibid.*, p. 16.

[55] V. Joubert et J.-L. Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE », *Hérodote*, n° 152-153, 2014/1, p. 262.

[56] Un cyberincident concerne « *tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information* » (*Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, p. 13).

[57] V. Joubert et J.-L. Samaan, *op. cit.*

[58] *Le Concept Stratégique de l'Alliance approuvé par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Washington les 23 et 24 avril 1999* (http:/www.nato.int/docu/pr/1999/p99-065f.htm).

cyberattaques »[59]. La problématique semble alors considérée comme « *anecdotique* »[60] ; elle est envisagée sous un angle technique, et elle ne suscite aucun sentiment d'urgence, qu'il soit politique ou stratégique[61].

Le début des années 2000 voit la mise en place d'une politique de cybersécurité par l'UE, qui s'appuie sur la création d'agences européennes spécifiquement dédiées à la cybersécurité et sur l'adoption de multiples directives européennes relatives aux technologies de l'information et de la communication[62]. Celles-ci s'inscrivent dans le droit fil des décisions juridiques de l'UE : la préservation des libertés individuelles des citoyens européens en protégeant les données relatives à leur identité, et la garantie de la poursuite et de la pérennité des activités commerciales et économiques électroniques par une sécurisation des technologies œuvrant aux transactions de biens[63]. D'après J-M. Bockel néanmoins, « *ces documents fixent des objectifs très généraux, mais ne paraissent pas encore en mesure de se traduire rapidement par des initiatives concrètes*»[64]. En 2003, la stratégie européenne de sécurité intitulée « *Une Europe sûre dans un monde meilleur* » n'inclut d'ailleurs pas encore les cyberattaques dans les « *nouvelles menaces* » auxquelles est confrontée l'Europe. À cette époque, l'UE semble davantage préoccupée par le terrorisme, la prolifération des armes de destruction massive, les conflits régionaux, la déliquescence des États et la criminalité organisée[65]. Sur ce dernier point, il faut reconnaître le rôle important joué par l'UE, lors de la signature de la convention internationale sur la cybercriminalité signée en 2001 à Budapest et négociée dans le cadre du Conseil de l'Europe. Ce document exige que les États parties criminalisent certaines infractions commises soit par le biais de moyens informatiques sur ou en provenance de leurs territoires, soit du fait de leurs propres ressortissants. Il oblige également les États parties à fournir une assistance mutuelle dans les enquêtes

---

[59] *Déclaration du Sommet de Prague diffusée par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord*, 21 novembre 2002, § 4) f. L'Alliance atlantique met en place, dès 2003, une structure spécifique destinée à protéger ses propres systèmes d'information et de communication : le centre technique de la capacité OTAN de réaction aux incidents informatiques (*Nato computer incident response capability - NCIRC*). Ce centre, en phase « *opérationnelle initiale* » en 2006, est entièrement opérationnel en 2013 (V. Joubert et J.-L. Samaan, *op. cit.*, p. 263).

[60] *Ibid.*, p. 265.

[61] *Ibid.*, p. 263.

[62] *Ibid.*, pp. 267-268. Une agence européenne chargée de la sécurité des réseaux et de l'information, l'ENISA (*European Network and Information Security Agency*) est créée, en mars 2004, dans le but de « *favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information* » au sein de l' l'Union européenne, « *prenant part ainsi au bon fonctionnement du marché intérieur* » (*Règlement (CE) n°460/2004 du Parlement européen et du Conseil du 10 mars instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information*, §15). Début décembre 2018, le Conseil et la Commission européenne sont parvenus à un accord politique concernant le règlement sur la cybersécurité, qui renforce le mandat de l'ENISA afin de soutenir davantage les États membres dans la lutte contre les cybermenaces et les et les cyberattaques. Ce règlement prévoit un mandat permanent pour l'ENISA, en remplacement de son mandat limité, lequel aurait expiré en 2020, ainsi que davantage de ressources allouées à l'Agence afin de lui permettre d'atteindre ses objectifs. Il envisage également une « *base plus solide pour l'Agence, sous la forme d'un nouveau cadre de certification de cybersécurité, afin d'aider les États memebres à réagir efficacement aux cyberattaques, assortie d'un rôle plus important dans la coopération et la coordination au niveau de l'Union* » (Communiqué de presse de la Commission européenne, « Les négociateurs de l'Union européenne décident de renforcer la cybersécurité en Europe », Bruxelles, 10 décembre 2018 (http://europa.eu/rapid/press-release_IP-18-6759_fr.htm, consulté le 12 décembre 2018).

[63] V. Joubert et J.-L. Samaan, *op.cit.*, p. 268.

[64] J.-M. Bockel, *Rapport d'information du Sénat*, n°681, 18 juillet 2012, p. 58.

[65] Note du Haut représentant de l'UE, *Une Europe sûre dans un monde meilleur. Stratégie européenne de sécurité*, Bruxelles, 12 décembre 2003, pp. 3-4.

et dans les poursuites[66]. Si 56 pays ont à ce jour ratifié la convention, un État comme la Russie n'a toujours pas jugé utile d'y apposer sa signature[67]. Par ailleurs, seuls deux pays membres de l'UE n'ont pas encore ratifié le document : l'Irlande et la Suède[68].

Les attaques informatiques qui frappent l'Estonie en 2007, puis la Géorgie en 2008 constituent un tournant dans l'histoire cybernétique. Elles consistent à utiliser les technologies de l'information et des communications pour parvenir à l'hégémonie politique et militaire, notamment en ayant recours à des moyens offensifs[69]. Selon N. Arpagian, les événements dont sont victimes ces États illustrent « *la première génération de cette forme annoncée de cyberguerre, lorsque les technologies de l'information et de la communication sont mises à contribution pour appuyer un jeu diplomatique et géopolitique bien réel* »[70]. Dans les deux cas, les principaux sites gouvernementaux de ces pays sont victimes d'« attaques en déni de service » et de « défacement ». Ils deviennent en effet inaccessibles et certaines pages d'accueil des sites ministériels se trouvent ornés d'insignes nazis.

De plus, dans le cas géorgien, les piratages numériques clouent alors au sol l'aviation militaire, soit une flotte de dix-huit appareils[71]. En définitive, les cyberattaques menées contre la Géorgie se révèlent beaucoup plus efficaces que celles perpétrée en Estonie pour une simple raison : leur concordance avec le rythme des manœuvres militaires russes[72]. Il s'agit du premier exemple d'une combinaison d'actions militaires classiques et cybernétiques. Les conséquences de ces cyberincidents restent cependant relativement limitées par rapport aux perturbations survenues en Estonie. Ceci s'explique principalement par la faible dépendance de la population géorgienne à l'Internet[73]. C'est à l'occasion du conflit russo-géorgien, et dans le prolongement de l'attaque informatique qui frappe l'Estonie en 2007, que les États membres de l'OTAN commencent à poser la question de savoir si des assauts informatiques peuvent ou non être assimilés à des interventions militaires classiques et, dès lors, entraîner l'application ou non de l'article 5 du traité fondateur de 1949[74]. Celui-ci prévoit que si un des membres de l'Alliance fait l'objet d'une « *attaque armée* », l'organisation atlantique doit lui venir en aide et éventuellement participer à la riposte. Néanmoins, malgré l'évocation de l'article 5 par l'Estonie en 2007, pays membre de l'UE et de l'OTAN, l'Alliance atlantique décide de ne pas intervenir, au vu de l'absence d'un texte officiel envisageant l'assimilation d'une cyberagression à une « attaque armée ».

---

[66] M. Fontaine et M. Benatar, « Cyber-attaques : aperçu du cadre juridique national », *Questions juridiques d'actualité en lien avec la défense*, 2017, pp. 319.-320

[67] La pensée stratégique russe actuelle ne reconnaît en effet aucunement l'existence d'un cyberespace qui serait un objet exclusif et incomparable requérant ses propres règles de gouvernance. Au contraire, « *elle estime que les réseaux numériques tels que l'Internet sont des médias parmi d'autres, sur lesquels l'État a ordinairement un droit de régulation. On devine alors que la conception russe est largement conditionnée par l'importance qu'attache son gouvernement à la question de la souveraineté, là où la notion de cyberespace tend à l'effacer* » (K. Limonier, « La Russie dans le cyberespace : représentations et enjeux », *Hérodote*, n° 152-153, 2014/1, p. 143).

[68] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

[69] *Communication de la commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions relative à la protection des infrastructures d'information critiques 'Réalisation et prochaines étapes : vers un cybersécurité mondiale'*, Bruxelles, 31 mars 2011 [COM (2011) 163 final], p. 3.

[70] N. Arpagian, *La cybersécurité, Que sais-je ?* 2010, p. 25.

[71] *Ibid.*, pp. 25-26.

[72] V. Joubert et J.-L. Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE », *Hérodote*, n° 152-153, 2014/1, p. 265.

[73] M. Fontaine et M. Benatar, « Cyber-attaques: aperçu du cadre juridique national », *Questions juridiques d'actualité en lien avec la défense*, 2017, p. 315.

[74] N. Arpagian, *La cyberguerre. La guerre numérique a commencé*, Paris, 2009, pp. 37-38.

D'après D. Ventre, les cyberattaques survenues à l'encontre de ces deux États baltes font office d' « *électrochoc pour la communauté internationale* »[75]. Il semble en effet acquis que l'on ne peut plus concevoir de conflit militaire sans que celui-ci s'accompagne d'attaques sur les systèmes d'information[76]. Il y a également une prise de conscience du fait que les cybermenaces guettent les infrastructures qui pilotent nos grands systèmes industriels : barrages hydroélectriques, centrales électriques ou nucléaires, stations de traitement des eaux, coordination des circulations aériennes ou ferroviaires[77]. À partir de ce moment, le sujet n'est plus seulement traité techniquement mais il fait partie intégrante de l'agenda politique de l'OTAN, qui adopte, en janvier 2008, sa première « politique de cyberdéfense »[78]. Celle-ci a pour objectif de renforcer la protection des systèmes d'information et de communication (SIC) de l'Alliance. Elle rappelle dans ce cadre que les pays membres sont responsables de la protection des extensions nationales des SIC de l'OTAN et des SIC qui leur appartiennent. Les systèmes d'information et de communication (SIC) nationaux qui remplissent des fonctions essentielles au sein d'un pays peuvent en effet revêtir une importance cruciale pour l'Alliance en cas de cyberattaque à l'échelle de tout un pays. L'Alliance s'engage également à mettre en place des capacités et des procédures visant à renforcer sa cyberdéfense et à aider, sur demande, les pays membres à contrer des cyberattaques d'ampleur nationale[79]. C'est dans ce cadre que l'OTAN ouvre, en mai 2008, un centre d'analyse et d'expertise en matière de cybersécurité (« Centre d'excellence de cyberdéfense coopérative de l'OTAN »). Situé dans la capitale estonienne, il mène des exercices mais également des activités de recherche et de formation dans des domaines techniques, juridiques et stratégiques liés à la cybersécurité[80]. En décembre 2008, l'UE émet quant à elle un rapport destiné à améliorer la mise en œuvre de la stratégie européenne de sécurité de 2003. En matière de cybersécurité, ce document recommande des travaux supplémentaires dans le domaine de la criminalité sur Internet afin d'envisager une approche globale de l'UE et de renforcer la coopération internationale[81].

---

[75] D. Ventre, « Les évolutions de la cybersécurité : contraintes, facteurs, variables… », *Étude Prospective et Stratégique*, n° 1506388759, juin 2015.

[76] J.-M. Bockel, *Rapport d'information du Sénat*, n°681, 18 juillet 2012, p. 36.

[77] N. Arpagian, *La cybersécurité, Que sais-je ?*, 2010, p. 26.

[78] V. Joubert et J.-L. Samaan, *op. cit.*, pp. 263-264.

[79] *Déclaration du Sommet de Bucarest publiée par les chefs d'État et de gouvernement participant à la réunion du Conseil e l'Atlantique Nord tenue à Bucarest le 3 avril 2008*, § 47. Le Bureau de gestion de la cyberdéfense de l'OTAN (CDMB) est créé en 2008 afin de coordonner des activités de cyberdéfense dans l'ensemble des organismes civils et militaires de l'OTAN. Le CDMB gère également en premier lieu et immédiatement les crises touchant à la cyberdéfense de l'Alliance et traite les situations susceptibles de s'aggraver rapidement (G. Le Bris et Ph. Vittel, *Rapport d'information de l'Assemblée nationale*, n°3472, 3 février 2016, p. 69 ; J.-M. Bockel, *Rapport d'information du Sénat*, n°681, 18 juillet 2012, p. 58).

[80] https://ccdcoe.org/about-us.html. Le centre d'excellence de cyberdéfense coopérative de l'OTAN situé à Tallinn a notamment permis la publication en 2013, du premier « *manuel de Tallinn* », étoffé depuis, qui œuvre à la transposition du droit international des conflits armés à des affrontements dans le cyberespace (https://ccdcoe.org/tallinn-manual.html, consulté le 17 décembre 2017)

[81] S.n., *Rapport sur la mise en œuvre de la stratégie européenne et de sécurité. Assurer la sécurité dans un monde en mutation*, Bruxelles, 11 décembre 2008 [S407/08], p. 5.

Le virus « Stuxnet » permet l'endommagement de centrifugeuses nucléaires

En avril 2010, l'OTAN est à nouveau la cible de plusieurs attaques informatiques attribuées, cette fois, à la mouvance *Anonymous*. L'ordinateur personnel du secrétaire général de l'OTAN est également piraté[82]. Deux mois plus tard, le programme nucléaire iranien, et plus précisément les installations d'enrichissement d'uranium de Natanz, font l'objet d'une attaque informatique de grande ampleur, dont l'origine serait israélo-américaine[83]. Cette opération provoque vraisemblablement l'endommagement de 1000 centrifugeuses suite à l'introduction du virus « Stuxnet » dans le système de contrôle de celles-ci. Il s'agit, à ce jour, de l'unique cas connu de cyberattaque ayant mené à la destruction physique d'équipements. En d'autres termes, les conséquences de cette opération sont similaires à celles d'une attaque conventionnelle[84].

C'est dans ce contexte très préoccupant que la problématique de la cyberdéfense apparaît comme un nouveau défi dans le concept stratégique de l'OTAN adopté en 2010, lors du Sommet de Lisbonne[85]. L'organisation y explique que les cyberattaques sont de plus en plus nombreuses et complexes, et que le montant des dégâts causés va croissant. Elle précise que ces menaces risquent d'atteindre *« un seuil pouvant menacer la prospérité, la sécurité et la stabilité des États et de la zone euro-atlantique* »[86]. Le risque de cybercriminalité et de cyberterrorisme est également évoqué[87]. L'OTAN s'engage dès lors à développer une capacité centralisée de cyberdéfense pour tous les organismes de l'OTAN. Celle-ci s'appuiera sur les moyens des Alliés pour faire face aux cybermenaces et sera destinée à « *prévenir et détecter les cyberattaques, à [s] en défendre et à [s'] en relever*»[88]. Quelques mois plus tard, en juin 2011, l'Alliance publie une nouvelle « politique OTAN de cyberdéfense ». Les objectifs et le plan d'action pour sa mise en oeuvre sont les mêmes que ceux fixés dans sa politique de cyberdéfense de 2008, à savoir mettre en place des capacités et procédures afin de renforcer la sécurité des systèmes d'information de l'Alliance et d'aider, sur demande, les Alliés qui seraient visés par une cyberattaque d'ampleur nationale[89]. Le document reste cependant très évasif quant à l'étendue de cette assistance[90]. Il propose néanmoins, chose nouvelle, l'institutionalisation de la dimension informatique au sein du

---

[82] J.-M. Bockel, *Rapport d'information du Sénat*, n°681, 18 juillet 2012, p. 59.

[83] G.-H. Soutou, « Éditorial», *Stratégique*, n°117, 2018, p. 10.

[84] M. Fontaine et M. Benatar, « Cyber-attaques : aperçu du cadre juridique national », dans *Questions juridiques d'actualité en lien avec la défense*, 2017, Bruxelles, p. 316. S. Taillat considère que les opérations numériques de décembre 2015 contre le système de distribution électrique ukrainien ont également entraîné des dommages physiques sur les infrastructures (S. Taillat, « Le cyberespace et la conflictualité internationale », dans S. Taillat, A. Cattaruzza et D. Danet, La Cyberdéfense. Politique de l'espace numérique, Paris, 2018, p. 27).

[85] *Concept stratégique pour la défense et la sécurité des membres de l'Organisation du Traité de l'Atlantique Nord adopté par les chefs d'État et de gouvernement à Lisbonne*, 19 novembre 2010, § 19.

[86] *Ibid.*, § 12-13.

[87] *Ibid.*, § 12.

[88] *Ibid.*, § 19.

[89] J.-M. Bockel, *Rapport d'information du Sénat*, n°681, 18 juillet 2012, p. 58. En 2012, l' « Agence OTAN d'information et de communication » (NCIA) est mise en place. Elle constitue le principal fournisseur de capacités C3 (consultation, commandement et contrôle) et prestataire de services SIC (systèmes d'information et de communication) de l'Alliance. Cette agence fournit en outre un soutien informatique au siège de l'OTAN, à la structure de commandement de l'OTAN et aux autres agences de l'OTAN (S.n., *Agence OTAN d'information et de communication*, 3 juillet 2012, www.nato.int).

[90] V. Joubert et J.-L. Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE », dans *Hérodote* 2014/1 (n°152-153), p. 265.

processus de planification de l'OTAN. Ainsi, anecdote significative, les exercices de crise conduits par le quartier général incorporent désormais un scénario de cyberattaques[91].

C'est au début des années 2010 que l'UE prend en considération l'impact que peuvent avoir les cyberattaques sur la défense et la sécurité nationale de ses États membres et, par conséquent, sur sa propre cybersécurité[92]. En septembre 2012, la *Computer Emergency Response Team* (CERT) UE voit le jour. Elle constitue le centre opérationnel en charge de la sécurité des systèmes d'information et réseaux de l'ensemble des institutions de l'UE. Cette CERT permet aux instances de l'UE d'étendre leur politique de cybersécurité pour la tourner vers les États membres, de manière à améliorer globalement le niveau de cybersécurité en Europe[93].

Les dangers de la cyberguerre [94] et du cyberterrorisme commencent à être évoqués dans les documents officiels de l'UE[95]. La possibilité que les cyberattaques puissent être exploitées par des mouvements terroristes en complément d'attentats réels pour les amplifier suscite une certaine inquiétude mais reste, à ce jour, peu vraisemblable. Selon J.-L Samaan en effet, « *le cyberespace et les systèmes de sécurité changent si rapidement que l'actualisation des techniques d'intrusion et de destruction devient un travail extrêmement coûteux, rendant une cyberattaque terroriste de grande envergure peu probable* »[96].

En février 2013, l'UE publie sa première stratégie de cybersécurité destinée à promouvoir un *« cyberespace ouvert, sûr et sécurisé »*[97]. Le développement d'une politique et de moyens de cyberdéfense liée à la politique de sécurité et de défense commune (PSDC) fera désormais partie des priorités stratégiques[98]. Néanmoins, pour éviter la redondance avec les activités et les capacités de cyberdéfense de l'OTAN, l'UE s'engage à étudier les différentes possibilités de conjuguer ses efforts avec ceux de l'Alliance afin d' « *accroître la résilience des infrastructures critiques d'État, de défense ou d'information dont dépendent les membres des deux organisations* »[99]. Outre la cyberdéfense, la cyberstratégie européenne s'articule autour de quatre autres priorités : la cyber-résilience, le recul de la cybercriminalité, le développement de ressources industrielles et technologiques en matière de

---

[91] *Ibid.*, pp. 266-267.

[92] Communication conjointe au Parlement européen, au Conseil, au comité économique et social européen et au Comité des régions. *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, février 2013 [JOIN (2013) 1 final], p. 12.

[93] V. Joubert et J.-L. Samaan, *op. cit*., p. 268.

[94] *The Concise Oxford English Dictionnary 2017* définit la cyberguerre comme « *the use of computers to dirupt the activities of an enemy country, especially the deliberate attacking of communication systems* ». C'est également la définition préconisée par l'OTAN (*NATO Terminology Directive-PO (2015) 0193*, 16 avril 2015, p. 4, § 1.3.2). O. Kempf utilise le terme de cyberguerre pour désigner « des actions hostiles menées dans le cyberespace par des États pour résoudre par la violence (maîtrisée) leurs conflits » (O. Kempf, *op. cit.*, p. 58)

[95] *Communication de la commission au Parlement européen, au Conseil, au comité économique et social européen et au Comité des régions relative à la protection des infrastructures d'information critiques' Réalisation et prochaines étapes : vers un cybersécurité mondiale'*, Bruxelles, 31 mars 2011 [COM (2011) 163 final], p. 3.

[96] J.-L Samaan, « Mythes et réalités des cyberguerres », dans *Politique étrangère*, n°4, 2008, p. 836.

[97] Communication conjointe au Parlement européen, au Conseil, au comité économique et social européen et au Comité des régions, *op. cit.*

[98] Communication conjointe au Parlement européen, au Conseil, au comité économique et social européen et au Comité des régions. *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, février 2013 [JOIN (2013) 1 final], p. 12.

[99] *Ibid.*

cybersécurité et une politique internationale du cyberespace conforme aux valeurs essentielles de l'UE[100].

La crise russo-ukrainienne ou le recours à des armes numériques sur fond de « guerre hybride »

En février 2014, le continent européen est à nouveau confronté à des cyberattaques de grande ampleur. Cette fois-ci, c'est l'Ukraine qui est visée. Lors de la crise russo-ukrainienne, la Russie aurait en effet mis en œuvre une série d'attaques cyber afin d'isoler la Crimée du gouvernement de Kiev[101]. Le comportement russe se caractérise ici, selon certains auteurs, par le recours à une « guerre de seuil » ou « guerre hybride » permettant de générer des effets stratégiques sans avoir à subir les conséquences d'une opération militaire en bonne et due forme[102]. De tels procédés peuvent profondément déstabiliser la communauté internationale, qui se voit dans l'incapacité de réagir, par la voie militaire notamment[103]. La « guerre hybride » englobe, lors de la crise ukrainienne, un certain nombre de pratiques relevant de la stratégie intégrale russe, caractérisée par le recours à un ou une combinaison de facteurs ambigus, tels que des cyberattaques, dont l'origine reste difficile à déterminer, mais aussi la possibilité de lancer une invasion de « petits hommes verts »[104] sans en subir de conséquences militaires en retour ainsi que le recours russe aux « proxys », forces agissant par procuration pour d'autres et soutenues militairement par ceux-ci[105].

Dans ce contexte de tensions internationales, l'OTAN adopte, en mai 2014, une troisième « politique de cyberdéfense », dont les lignes essentielles sont dévoilées dans le texte de la déclaration du sommet du Pays de Galles, publié quelques mois plus tard. Le document évoque l'importance pour l'OTAN d'être en mesure de « *faire face efficacement aux défis spécifiques posés par les menaces que présente la guerre hybride, dans le cadre de laquelle un large éventail de mesures militaires, paramilitaires ou civiles, dissimulées ou non, sont mises en œuvre de façon très intégrée* »[106]. Dans ce contexte, l'Alliance considère que l'impact des cyberattaques « *sur les sociétés modernes pourrait être tout aussi néfaste que celui d'une attaque conventionnelle* » et affirme dès lors qu' « *il reviendrait au Conseil de l'Atlantique Nord de décider, au cas par cas, des circonstances d'une invocation de l'article 5 à la suite d'une cyberattaque* »[107] , comme il le ferait en cas d'agression armée. Or la réponse juridique à donner à une cyberopération dépend de deux conditions, à savoir, d'une part, la violation d'une règle

---

[100] *Ibid.*, p. 5.

[101] J.-Ch. Coste, « *De la guerre hybride à l'hybridité cyberélectronique* », *Revue Défense Nationale*, Paris, mars 2016, p. 19.

[102] J. Henrotin, « La guerre hybride comme avertissement stratégique », dans *Stratégique*, n°111, Paris, 2016, p. 20.

[103] *Letter of the Defence Policy Directors of 10 Northem Group Nations to EEAS DSG Maciej Popowsk*i, 17 février 2015.

[104] Les « *petits hommes verts* », forces spéciales russes sans insignes observées en Crimée, ne permettaient pas une identification correcte, ni la qualification en bonne et due forme d'une agression. Il s'agissait *in fine* de manœuvrer en se servant d'une interprétation du droit international (J. Henrotin, « La guerre hybride comme avertissement stratégique», *Stratégique*, n°111, Paris, 2016, pp. 19-20 ; E. Tenenbaum, « La manœuvre hybride dans l'art opératif », *Stratégique*, n°111, Paris, 2016, p. 52)

[105] E. Tenenbaum, *op. cit.*, p. 20, pp. 19-20.

[106] *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 les 4 et 5 septembre 2014*, 7 septembre 2014, § 13.

[107] *Ibid.*, § 72.

du droit international et, d'autre part, la possibilité d'attribuer l'action à un auteur[108]. Déterminer juridiquement si une cyberattaque peut être considérée comme une agression armée n'est pas chose aisée et ne fait pas l'unanimité[109]. La question de l'attribution est également compliquée pour deux autres raisons. D'une part, l'origine de l'attaque est techniquement complexe à déterminer. D'autre part, il est difficile de prouver qu'une cyberattaque est le fait d'un individu et/ ou d'un État.

Pour certains, le concept de cyberattaque ne requiert pas le recours à la force[110]. En outre, d'aucuns considèrent que la question de l'attribution d'une opération cybernétique reste insoluble à ce jour[111]. Il semble dès lors que la décision éventuelle d'intervenir au nom de l'article 5, serait en définitive politique et reviendrait au Conseil de l'Atlantique Nord, dans le respect du droit international. Par ailleurs, d'un point de vue opérationnel cette fois, les débats ne manquent pas sur la manière de répondre à une cyberattaque. Faut-il y riposter par une contre-attaque informatique (pratique du « *hack-back* » ou de la « cyberdéfense active »[112]) et/ou par une réponse conventionnelle ?[113] Ou doit-on au contraire privilégier la « cyberdiplomatie »[114] avant d'envisager, en dernier recours, une riposte ?

En juin 2017, l'UE réaffirme dans un document intitulé « Boîte à outils cyberdiplomatiques » qu' « *elle est attachée au règlement des différends internationaux dans le cyberespace par des moyens pacifiques, et que l'ensemble des efforts diplomatiques déployés par l'UE devraient en priorité être axés sur la promotion de la sécurité et de la stabilité dans le cyberespace au moyen d'une coopération internationale renforcée, ainsi que sur la réduction du risque de perceptions erronées, d'escalade et de conflits qui peuvent découler d'incidents liés aux TIC* »[115].

Quoi qu'il en soit et compte tenu des difficultés d'attribution ainsi que du rôle important des acteurs privés, le droit international permet aux États, grâce à l'obligation de diligence (*due diligence*)[116],

---

[108] M. Fontaine et M. Benatar, « Cyber-attaques: aperçu du cadre juridique national », dans *Questions juridiques d'actualité en lien avec la défense*, 2017, Bruxelles, p. 342.

[109] *Ibid.*, pp. 320-321, 341.

[110] *Ibid.*, p. 341.

[111] *Ibid.*, pp. 322, 341.

[112] Le terme de « *hack-back*» ou « *hacking back* » ne connaît pas vraiment de définition officielle mais pourrait être traduit en français par « contre piratage ». Il décrit le fait, pour une victime d'une cyberattaque, de riposter contre son auteur. On a toutefois tendance à préférer l'emploi d'un néologisme, celui de « cyberdéfense active » qui permet d'apporter un fort degré de légitimation à la réaction de la victime en renvoyant de manière implicite au concept juridique de la « légitime défense ». Cette expression occulte par ailleurs le caractère offensif des mesures adoptées : il ne s'agit pas d'une contre-offensive mais d'une « défense active » (K. Bannelier et Th. Christakis, Cyberattaques. « Prévention-réactions : rôle des États et des acteurs privés », *Les Cahiers de la Revue Défense Nationale*, pp. 61-62).

[113] V. Joubert et J.-L. Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE », dans *Hérodote* 2014/1 (n°152-153), p. 264.

[114] La cyberdiplomatie est un terme relativement nouveau qui signifie « *the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace* » (A. Barrinha et Th. Renard, « Cyber-diplomacy: the making of an international society in the digital age », *Global Affairs*, 3 janvier 2018, p. 3).

[115] Conseil de l'Union européenne, *Conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique")*, Bruxelles, 19 juin 2017, p. 3 (http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/fr/pdf, consulté le 2 janvier 2019)

[116] L'UE souligne en effet que « *les activités cybermalveillantes sont susceptibles de constituer des actes illicites au regard du droit international et rappelle que les États ne devraient pas mener ou soutenir sciemment des activités informatiques contraires aux obligations qui leur incombent en vertu du droit international, et qu'ils ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide*

d'engager la responsabilité internationale d'un pays à partir du territoire duquel une cyberopération portant atteinte aux droit de l'État victime a été lancée. L'interprétation et la mise en œuvre de cette obligation constituent un défi majeur dans l'application du droit international aux cyberopérations[117]. L'État victime pourrait ainsi s'adresser au Conseil de sécurité des Nations unies pour faire qualifier la cyberattaque de menace contre la paix. Dans l'éventualité d'un acte d'agression, l'État victime peut réagir sur base de la légitime défense[118]. Il pourrait également décider de saisir la Cour internationale de justice pour que les pays qui commettent des cyberattaques voient leur responsabilité engagée et puissent éventuellement être condamnés. L'État victime aurait également la possibilité de décider le recours à des mesures unilatérales extrajudiciaires ou à des mesures de contrainte, légalement contestables, afin d'exercer une pression sur d'autres pays pour répondre à des actes ou des omissions de la part des États visés[119]. En juin 2018, le Parlement européen constatait la « *pertinence du manuel de Tallinn 2.0*[120] *comme point de départ pour débattre et comme analyse des modalités d'application du droit international en vigueur dans le cyberespace (…) [et signalait] en particulier que toute utilisation offensive de cybercapacités devrait reposer sur le droit international* »[121].

Á cet égard, il convient de noter que le secrétaire général de l'OTAN Jens Stoltenberg a déclaré, le 8 novembre 2017, que les ministres de la défense de l'OTAN ont donné le feu vert à l'utilisation de leurs capacités offensives en matière de cyberguerre lors des opérations de l'Alliance. Les pays qui disposent de telles capacités restent néanmoins souverains dans la mise en œuvre de celles-ci. Les tactiques de cyberguerre pour intercepter des échanges, éteindre des serveurs ou saboter des technologies utilisées au combat auraient d'ailleurs déjà été utilisées en Irak et en Syrie contre le groupe « État islamique » par des pays de l'Alliance[122]. Étant donné les cyber-capacités offensives de certains d'entre eux, il serait intéressant que l'OTAN développe un scénario stratégique purement cyber, dans lequel l'Alliance serait habilitée à recourir à des méthodes exclusivement cyber offensives pour contrer de possibles cyberattaques contre ses propres systèmes d'information et de communication et/ou les CIS nationaux d'un ou plusieurs pays alliés. Certains experts proposent d'ailleurs de transposer le concept stratégique de riposte graduée, adopté en 1967 par l'OTAN et initialement destiné au risque nucléaire, au champ cybernétique[123]. La mise en place d'un tel scénario pourrait en tout cas jouer un rôle de dissuasion important. Dans cette optique, la récente création d'un « centre d'opérations cyber » à l'OTAN

---

des technologies de l'information et des communications, comme indiqué dans le rapport de 2015 du groupe d'experts gouvernementaux des Nations unies » (*Ibid.*, p. 3).

[117] F. Delerue et A. Géry, « Les aspects juridique et stratégique de la cyberdéfense », dans S. Taillat, A. Cattaruzza et D. Danet, *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2018, p. 69.

[118] « *La légitime défense est le dernier seuil de mesures extrajudiciaires. Un État victime d'une agression armée au sens de l'Article 51 de la Charte des Nations unies peut invoquer son droit de légitime défense, et prendre des mesures incluant le recours à la force* » (*Ibid*.)

[119] *Ibid.*

[120] La deuxième édition du manuel de Tallinn, publiée en 2017 (« manuel de Tallinn 2.0 ») et rédigée, comme le manuel de Tallinn 2013 (1ère édition), sous les auspices du « centre d'excellence de cyberdéfense coopérative de l'OTAN », par un groupe d'experts académiques sous la direction du Professeur Michael Schmitt, expose un certain nombre de règles d'interprétation du droit international applicables aux cyberopérations, qui font l'objet d'un certain consensus et sont accompagnées de commentaires précisant la position des experts permettant de les interpréter et de les mettre en pratique (F. Douzet et S. Taillat, « Les enjeux de politique internationale. L'affirmation du leadership américain », dans S. Taillat, A. Cattaruzza et D. Danet, *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2018, p. 118).

[121] *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense*, 2018, § 47.

[122]Agence France Presse (AFP), « L'OTAN parée pour la cyberguerre », Bruxelles, 8 novembre 2017 (https://www.tdg.ch/monde/L-OTAN-paree-pour-la-cyberguerre/story/28222439, consulté le 15 janvier 2018).

[123] B. Gruselle, B. Tertrais et A. Esterle, « Cyberdissuasion », *Recherches & documents*, n°03/2012, p. 53.

constitue une étape cruciale dans l'intégration des capacités cybernétiques à la planification des opérations de l'Alliance [124].

En novembre 2014, l'UE publie quant à elle un document destiné à fournir un « cadre d'action en matière de cyberdéfense », conformément aux recommandations préconisées par sa stratégie de cybersécurité de 2013. Dans ce texte, l'UE énumère 5 priorités. Primo, elle s'engage à aider les États membres à développer des « *capacités de cyberdéfense solides et résilientes (…) pour soutenir les structures, les missions et les opérations PSDC* »[125]. Secundo, elle déclare vouloir renforcer la protection des réseaux de communication de la PSDC utilisées par les entités européennes[126]. Dans ce cadre, l'UE prévoit d'élaborer un « *concept unifié sur la cyberdéfense pour les opérations militaires et les missions civiles PSDC* » qui sera intégré dans la planification au niveau stratégique[127]. Tertio, elle recommande la coopération civilo-militaire en matière de cybersécurité et de défense, au vu du rôle essentiel joué par les « *capacités à double usage* » [128] dans le domaine du cyberespace[129]. Quarto, l'UE s'engage à améliorer les possibilités de formation et d'exercice en matière de cyberdéfense pour les acteurs militaires et civils de la PSDC[130]. *Last but not least*, elle annonce le renforcement de la coopération avec les partenaires internationaux concernés par les problèmes de cyberdéfense, comme l'ONU et l'OSCE[131]. Ces deux organisations s'efforcent en effet, depuis quelques années, d'établir des règles dans le cyberespace[132]. Par ailleurs, l'UE désire renforcer sa coopération en matière de cyberdéfense avec l'OTAN. L'objectif est clair : assurer la cohérence et la complémentarité des efforts déployés par les

[124] https://www.nato.int/cps/ic/natohq/news_148722.htm?selectedLocale=fr, consulté le 15 janvier 2018.

[125] Conseil de l'Union européenne, *Cadre d'action de l'UE en matière de cyberdéfense*, Bruxelles, 18 novembre 2014 [15585/14], p. 2.

[126] *Ibid.*, p. 6.

[127] *Ibid.*, p. 7.

[128] *Ibid.*, p. 3.

[129] *Ibid.*, p. 8. Ainsi par exemple, il est primordial d'entretenir une coopération étroite entre les institutions et agences compétentes liées à la PSDC avec l'industrie dans le domaine de la technologie et de l'innovation liées à la cyberdéfense (*Ibid.*, p.9).

[130] Conseil de l'Union européenne, *Cadre d'action de l'UE en matière de cyberdéfense*, Bruxelles, 18 novembre 2014 [15585/14], pp. 11-12.

[131] En 2013 et en 2015, deux rapports (UNGGE- *UN Group of Governemental Experts*) avalisés par l'assemblée générale des Nations unies ont reconnu des principes généraux liés au respect du droit international dans le cyberespace (K. Bannelier et Th. Christakis, Cyberattaques. « Prévention-réactions : rôle des États et des acteurs privés », *Les Cahiers de la Revue Défense Nationale*, pp. 8, 15). Le rapport de 2013 reconnaît l'applicabilité de la Charte des Nations unies dans l'espace numérique et celui de 2015 contient des « *normes de comportement responsable des États* » afin de renforcer la stabilité de l'espace cybernétique. La dernière assemblée des groupes d'experts gouvernementaux (GGE) de juin 2017, qui donnait pour objectif aux États de clarifier et d'opérationnaliser le rapport de 2015, s'est soldé par un échec. Certains pays auraient alors proposé d'atténuer la distinction du seuil, ouvrant ainsi la voie à une acceptation plus large de la notion d'agression armée et étendant les situations dans lesquelles le droit de légitime défense pourrait être invoqué. Les États n'ont cependant pas pu parvenir à un consensus en la matière et aucun rapport n'a dès lors pu être adopté. (F. Delerue et A. Géry, « Les aspects juridique et stratégique de la cyberdéfense », dans S. Taillat, A. Cattaruzza et D. Danet, *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2018, p. 63). Selon A. Gery, « *cet échec illustre les profondes divergences entre les États tant en matière d'interprétation du droit international (notamment sur la légitime défense et les contre-mesures), que de perception des menaces et priorités stratégiques, et soulève par conséquent la question de l'avenir des négociations internationales* » (A. Gery, « La diplomatie du numérique », *Sécurité & Défense Magazine*, 23 janvier 2018, https://sd-magazine.com/securite-numerique-cybersecurite/la-diplomatie-du-numerique, consulté le 13 novembre 2018).

[132] Conseil de l'Union européenne, *Cadre d'action de l'UE en matière de cyberdéfense*, Bruxelles, 18 novembre 2014 [15585/14], p. 13.

deux organisations, tout en évitant d' « *inutiles doubles emplois* »[133] . Ainsi par exemple, elle s'engage, dans le respect de l'autonomie décisionnelle de l'UE, à mettre en commun « *les meilleures pratiques* »[134] en la matière, inspirées par la gestion de crise ainsi que les opérations et missions militaires ; à viser la cohérence dans l'élaboration des besoins de capacités en termes de cyberdéfense ; à renforcer la coopération en matière de formation et d'exercices entre l'UE et l'OTAN[135] ; et enfin, à échanger des informations sur les cybermenaces qui pourraient affecter les deux organisations[136]. Pour terminer, le « cadre d'action » de 2014 invoque la possibilité d'appliquer, le cas échéant, certaines dispositions juridiques pertinentes du traité UE et du traité sur le fonctionnement de l'UE « *afin de faire face aux conséquences d'une crise dans le domaine de la cybersécurité*»[137].

En effet, conformément à l'article 51 de la charte des Nations unies, si une cyberattaque constitue une agression armée[138] contre un État membre de l'UE, la clause d'assistance mutuelle de l'article 42, paragraphe 7 du TUE (Traité sur l'Union européenne)[139] pourrait être invoquée afin d'apporter une réponse appropriée en temps utile [140]. La clause de solidarité, décrite dans l'article 222 TFUE (Traité sur le fonctionnement de l'Union européenne) et relative aux attaques terroristes[141] ou catastrophes

---

[133] *Ibid.*, p. 13.

[134] En février 2016, un arrangement technique entre la NCIRC (*Nato computer incident response capability)* et le centre d'alerte et de réaction aux attaques informatiques de l'UE (CERT-UE) a été conclu entre les deux organisations. Il fixe un cadre pour l'échange d'informations et le partage de meilleures pratiques entre les équipes d'intervention d'urgence (S.n., « L'OTAN et l'Union européenne renforcent leur coopération en matière de cyberdéfense », 10 février 2016, https://www.nato.int/cps/fr/natohq/news_127836.htm, consulté le 21 janvier 2019).

[135] L'OTAN et l'UE commencent à intégrer les cyberattaques dans leurs exercices annuels de gestion de crises qui ont désormais lieu dans un environnement fictif de menaces hybrides. Le premier entraînement impliquant les deux organisations, toujours dans un scénario d'attaque hybride, a eu lieu en septembre- octobre 2017 (P Commission européenne, *Rapport conjoint au Parlement européen et au Conseil sur la mise en œuvre du 'cadre commun en matière de lutte contre les menaces hybrides- une réponse de l'Union européenne'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], pp. 18-19).

[136] Conseil de l'Union européenne, *Cadre d'action de l'UE en matière de cyberdéfense*, Bruxelles, 18 novembre 2014 [15585/14], p. 13.

[137] *Ibid.*, p. 3.

[138] La résolution 3314 des Nations Unies du 14 décembre 1974 définit une « *agression armée* » comme *« l'emploi de la force armée par un État contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un autre État, ou de toute autre manière incompatible avec la Charte des Nations Unies (…)* » (article premier de la résolution 3314 de l'Assemblée générale des Nations Unies du 14 décembre 1974).

[139] Comme dit dans article 42§7 du traité sur l'Union européenne: « *Au cas où un État membre serait l'objet d'une agression armée sur son territoire, les autres États membres lui doivent aide et assistance par tous les moyens en leur pouvoir, conformément à l'article 51 de la charte des Nations unies. Cela n'affecte pas le caractère spécifique de la politique de sécurité et de défense de certains États membres. Les engagements et la coopération dans ce domaine demeurent conformes aux engagements souscrits au sein de l'Organisation du traité de l'Atlantique Nord, qui reste, pour les États qui en sont membres, le fondement de leur défense collective et l'instance de sa mise en œuvre* » (« Traité sur l'Union européenne (version consolidée) », 2012, disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:12012M/TXT , consulté le 2 janvier 2019).

[140] *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2008/2004 (INI))*, § D.

[141] L'UE définit les infractions terroristes comme des « *actes intentionnels (…) qui, par leur nature ou leur contexte, peuvent porter gravement atteinte à un pays ou à une organisation internationale lorsque l'auteur les commet dans le but de gravement intimider une population ou contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque ou gravement déstabiliser ou détruire les structures fondamentales politiques, constitutionnelles, économiques ou sociales d'un pays ou une organisation internationale (…)* » (article premier de la *Décision cadre du Conseil du 13 juin 2002 relative à la lutte contre le*

naturelles ou d'origine humaine dont un pays de l'UE pourrait être victime[142], *« complète la clause de défense mutuelle en prévoyant que les États membres de l'Union sont tenus d'agir conjointement lorsque l'un d'eux est victime d'une attaque terroriste ou d'une catastrophe naturelle ou d'origine humaine »*[143]. Le Parlement européen est d'ailleurs conscient que « *compte tenu de l'environnement en mutation des cybermenaces, il est souhaitable de mettre en place une coopération renforcée et plus structurée avec les forces de police, notamment dans certains domaines critiques tels que la lutte contre des menaces comme le cyberdjihad [ou] le cyberterrorisme (…)* »[144].

Selon M. De Bruycker, il conviendrait de mettre en place un cadre normatif paneuropéen et/ou international unifié de cybersécurité afin d' « *éviter de mettre en œuvre des normes différentes d'un secteur à l'autre et d'un pays à l'autre* »[145].

« Hyper War via cyber War »?

Plus récemment, dans leur déclaration commune, signée à Varsovie en juillet 2016, l'UE et l'OTAN ont réaffirmé leur volonté d'approfondir leur coopération dans le domaine de la cybersécurité et de la cyberdéfense. Elles continuent à considérer que leur sécurité est « *interconnectée* » et qu'elles peuvent mobiliser ensemble un large éventail d'outils afin de répondre aux nouveaux défis sécuritaires[146]. Parmi ceux-ci, certains mettent en garde contre la technologie du cyber combat autonome (« *automating Cyber Operations* »[147]). D'aucuns recommandent en outre à l'OTAN d'envisager le danger de l' « *Hyper War via Cyber War* » dans son prochain concept stratégique[148]. Selon cette théorie, les guerres tendent en effet à s' « *automatiser* » et à voir leurs « *cycles de décision-actions considérablement raccourcis* », ce qui favorise le passage d'une situation de « *chaos à [celle de] capitulation* »[149].

---

terrorisme, disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32002F0475, consulté le 2 janvier 2019).

[142] L'article 222 du traité sur le fonctionnement de l'Union européenne dispose que « *l'Union et ses États-membres agissent conjointement dans un esprit de solidarité si un État-membre est l'objet d'une attaque terroriste ou la victime d'une catastrophe naturelle ou d'origine humaine. L'Union mobilise tous les instruments à sa disposition, y compris les moyens militaires mis à sa disposition par les États-membres, pour (…) porter assistance à un État membre sur son territoire, à la demande de ses autorités politiques (…)* » (« Traité sur le fonctionnement de l'Union européenne (version consolidée) », 2012 disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A12012E%2FTXT , consulté le 2 janvier 2019).

[143] *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2008/2004 (INI))*, § D.

[144] *Ibid.*, § 62.

[145] S.n., « La Cybersécurité : nous sommes tous concernés », [2017] (https://www.febelfin.be/fr/newsletter360/9/table-ronde-complete, consulté le 15 janvier 2019).

[146] *Joint Declaration by the President of the European Council, The President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, Varsovie, 8 juillet 2016.

[147] S. De Spiegeleire, M. Maas et T. Sweijs, *Artificial Intelligence and The Future of Defense. Strategic Implications for Small and Medium-Sized Force Providers*, La Haye, 2017, p. 87.

[148] J. Allen, Ph. M. Breedlove, J. Lindley-French et G. Zambellas, *Future War NATO? From Hybrid War to Hyper War via Cyber War. Supporting Paper of the GLOBSEC NATO Adaptation Initiative*, 2017, p. 15. Le concept d'« hyper-guerre » apparaît dès le début des années 1990, afin de rendre compte des conséquences de l'automatisation du combat (J. Henrotin, « Cyberdéfense : une généalogie », dans S. Taillat, A. Cattaruzza et D. Danet, *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2018, p. 72).

[149] J. Allen, Ph. M. Breedlove, J. Lindley-French et G. Zambellas, *op. cit.*, p. 7.

Par ailleurs et au vu de « *l'évolution et l'assombrissement constants du paysage des menaces* »[150], la cyberstratégie européenne de 2013 a été révisée en septembre 2017. Le nouveau document, surnommé « Paquet Cybersécurité 2017 » fixe trois priortiés : la cyber-résilience, la dissuasion par un renforcement des moyens d'identification et de répression et enfin, la défense grâce à un affermissement de la coopération internationale, notamment avec l'OTAN[151]. En juin 2018, le Parlement européen déclarait envisager la possibilité pour l'UE de rejoindre le Centre d'excellence pour la cyberdéfense de l'OTAN « *afin d'améliorer la complémentarité et la collaboration* »[152] entre les deux organisations. Il estime également qu'il est « *essentiel que l'Union et l'OTAN intensifient le partage de renseignements afin de permettre l'attribution formelle des cyberattaques et, par conséquent, d'imposer des sanctions restrictives aux responsables* »[153]. L'UE aimerait également s'engager dans le cyberpartenariat OTAN-industrie (NICP-*Nato Industry Cyber Partnership*)[154] établi en 2014 « *afin de créer un lien entre la coopération qu'elle a avec l'OTAN et les leaders spécialisés dans les cybertechnologies pour améliorer la cybersécurité grâce à une collabodation continue (…)* »[155].

Le Parlement européen souligne néanmoins « *la nécessité d'instaurer une terminologie plus claire concernant la sécurité dans le cyberespace* »[156]. G. Lasconjarias reconnaît également l'absence d'une définition commune de ce qu'est le cyberespace ou le cyberdomaine, « *autorisant un flou sur la nature profonde du cyber et donc, sur les activités qui y sont corrélées* »[157].

Malgré le travail des Alliés et de l'Union européenne en faveur du renforcement de la cybersécurité dans la région euro-atlantique et la coopération OTAN-UE en matière de cyberdéfense, les États restent des acteurs clés dans la protection des systèmes d'information et dans la réponse stratégique à apporter en cas de cyberattaque.

Le rôle des États dans le cyberespace euro-atlantique

Lors du Sommet de Varsovie, les chefs d'État et de gouvernement des pays de l'Alliance se sont engagés à faire du renforcement et de l'amélioration des moyens de cyberdéfense des infrastrucutres et des réseaux nationaux une priorité. Les États alliés sont dès lors tenus d'évaluer annuellement leur

---

[150] Communication conjointe au Parlement européen et au Conseil, *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017, p. 3 [JOIN (2017) 450 final]. Selon certaines études, l'incidence économique de la cybercriminalité a quintuplé entre 2013 et 2017, et pourrait quadrupler encore d'ici à 2019 (*Ibid.*, p. 2).

[151] D. Danet, « Collapsologie numérique », *Stratégique*, n°117, 2018, p. 216.

[152] *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense*, 2018, § 36.

[153] *Ibid.*, § 37.

[154] Le partage de l'information, les exercices communs, l'entraînement et la formation sont quelques exemples de domaines dans lesquels l'OTAN et l'industrie collaborent. Ce cyberpartenariat permet à l'OTAN de protéger ses propres réseaux, améliorer sa résilience et aider les Alliés à développer leurs capacités (https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_11/20171128_1711-factsheet-cyber-defence-fr.pdf, consulté le 2 janvier 2019).

[155] *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense*, 2018, § 43.

[156] *Ibid.*, § 14.

[157] G. Lasconjarias, « L'Otan et le domaine opérationnel cyber », dans S. Taillat, A. Cattaruzza et D. Danet, *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2018, pp. 150-151.

engagement en faveur de la cyberdéfense. Les résultats obtenus sont alors analysés afin de « *[renforcer] le dispositif de cyberdéfense et la résilience globale de l'Alliance* »[158].

Quelques jours après Varsovie, l'UE a quant à elle adopté la « directive SRI »[159] relative à la sécurité des réseaux et des systèmes d'information, qui impose des mesures de renforcement de la cybersécurité des États membres. Il s'agit du premier acte législatif concernant la cybersécurité à l'échelle de l'UE. Cette directive vise à « *renforcer la résilience en améliorant les capacités nationales en matière de cybersécurité, à favoriser une meilleure coopération entre les États membres et à exiger des entreprises actives dans des secteurs économiques importants qu'elles adoptent des pratiques efficaces de gestion des risques et signalent des incidents graves aux autorités nationales. Ces obligations s'appliquent également à trois types de fournisseurs de services internet clés : l'informatique en nuage*[160]*, les moteurs de recherche et les places de marché en ligne* »[161].

Les trois objectifs principaux de la directive SRI sont premièrement, la mise en place par tous les pays membres d'un minimum de moyens nationaux en matière de cybersécurité par l'institution d'autorités compétentes dans le domaine et l'adoption de stratégies et de plans de coopération en matière de SRI ; deuxièmement, le développement, par les autorités compétentes, d'un réseau permettant un échange coordonné d'informations ainsi que la détection des menaces cybernétiques, et facilitant, au niveau de l'UE, les interventions face aux menaces et incidents sur la SRI ; troisièmement, le partage d'informations entre le secteur privé et le secteur public pour permettre la mise en place de mesures appropriées et proportionnées afin de garantir la SRI et signaler aux autorités compétentes tout incident de nature à compromettre sérieusement leurs systèmes informatiques et susceptible d'avoir un impact significatif sur la continuité des services critiques et la fourniture des biens[162]. La directive s'applique

---

[158] S.n. « Engagement ern faveur de la cyberdéfense, 8 juillet 2016, §5 (https://www.nato.int/cps/fr/natohq/official_texts_133177.htm, consulté le 7 novembre 2018).

[159] La directive SRI ou NIS (for *Network and Information Security*) (« Directive (UE) 2016/1148 du parlement européen et du conseil du 6 juillet concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information », dans l'Union, dans le *Journal officiel de l'Union européenne*, 19 juillet 2016).

[160] L'« informatique en nuage » ou « cloud computing » en anglais est un système de stockage, de traitement et de mutualisation de données numériques, qui est apparu en 2006-2008 en réponse aux nouveaux défis informatiques que pose la digitalisation progressive des sociétés modernes (C. Bômont, « Maîtriser le *cloud computing* pour assurer sa souveraineté », dans S. Taillat, A. Cattaruzza et D. Danet, *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2018, p. 92).

[161] Communication conjointe au Parlement européen et au Conseil. *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017 [JOIN (2017) 450 final], p. 8.

[162] Proposition de résolution visant à renforcer la cybersécurité en Belgique, Chambre des représentants de Belgique, 16 septembre 2014, DOC 54 0257/001, p. 5.

aux opérateurs de « services essentiels »[163] et aux fournisseurs de services numériques[164]. Les États membres sont dès lors chargés d'établir quelles sont les entités qui remplissent les critères de la définition d'un opérateur de services essentiels[165]. Il était prévu que les pays membres adoptent et publient, au plus tard le 9 mai 2018, les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive[166].

Une sécurisation des CIS nationaux non suffisamment zélée est susceptible de porter atteinte à l'exécution des tâches fondamentales de l'UE et de l'OTAN, un constat qui s'applique également aux compagnies privées, contrôlant actuellement une grande partie du cyberespace. La coopération et l'échange d'informations entre le secteur public et le secteur privé reste néanmoins difficile. Les gouvernements et les autorités publiques sont en effet réticents lorsqu'il s'agit de partager des informations pertinentes pour la cybersécurité par crainte de compromettre la sécurité ou la compétititvité de leurs pays respectifs. Par ailleurs, d'aucuns considèrent que les entreprises privées « *rechignent quant à elles à partager des informations sur leurs failles en matière de cybersécurité et les pertes qui en résultent par crainte de compromettre des informations commerciales sensibles, de mettre en péril leur réputation ou de risquer d'enfreindre des règles en matière de protection des données* »[167]. La mise en oeuvre de la directive SRI devrait donner un « coup d'accélérateur » au partenariat public-privé en matière de cybersécurité[168].

Si la nature transfrontalière de la menace cyber plaide nettement en faveur d'une action multinationale, les États demeurent donc les premiers responsables de leur sécurité nationale[169].

---

[163] Un opérateur de service essentiel est une « *entité [qui] fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques ; la fourniture de ce service est tributaire des réseaux et des systèmes d'informations ; et un incident aurait un effet disruptif important sur la fourniture dudit service* ». (Directive (UE) 2016/1148 du parlement européen et du conseil du 6 juillet concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dans *Journal officiel de l'Union européenne*, 19 juillet 2016, p. 14). Plus concrètement, les services essentiels sont les secteurs d'infrastructures critiques (énergie, transports, banques et infrastrucutures numériques) mais également les secteurs liés aux marchés financiers, à la santé et à la fourniture et distribution d'eau potable (*Ibid*., pp. 27-29 ; *Proposition de résolution visant à renforcer la cybersécurité en Belgique*, Chambre des représentants de Belgique, 16 septembre 2014, DOC 54 0257/001, p. 6 ; *Rapport d'audition sur la cybersécurité des centrales nucléaires en Belgique*, Chambre des représentants de Belgique, 20 janvier 2017, DOC 54 2274/001, p. 4).

[164] « Directive (UE) 2016/1148 du parlement européen et du conseil du 6 juillet concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information », dans l'Union, dans le *Journal officiel de l'Union européenne*, 19 juillet 2016, p. 2.

[165] *Ibid.*, p. 4.

[166] *Ibid.*, p. 25. En juillet 2018, seuls 11 États membres avaient notifié à la Commission européenne la transposition intégrale de la directive NIS (https://www.nextinpact.com/news/106881-cybersecurite-france-epinglee-pour-defaut-transposition-integrale-directive-nis.htm, consulté le 29 décembre 2018).

[167] Communication conjointe au Parlement européen et au Conseil. *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017 [JOIN (2017) 450 final], p. 8.

[168] *Ibid.*, pp.8-9.

[169] Communication conjointe au Parlement européen et au Conseil. *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017, p. 3 [JOIN (2017) 450 final],

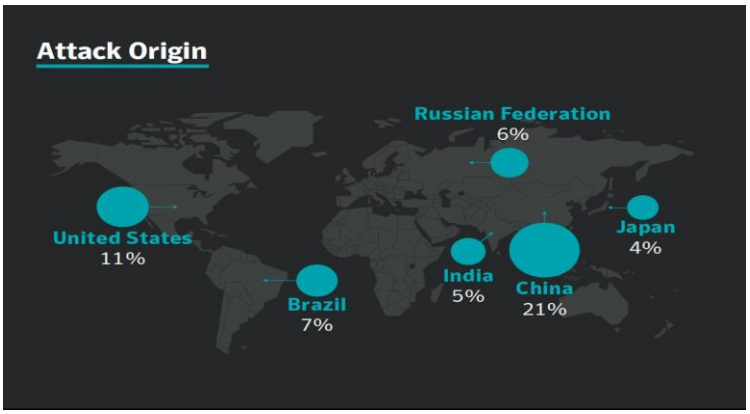
Défis et critères d'évaluation des cyberpuissances

Évolution chiffrée des cyberagressions et nouveaux enjeux

La cybersécurité est essentielle pour la prospérité et la sécurité des États, des entreprises privées mais également des organisations internationales. Néanmoins, rares sont les études liées à l'évolution des cyberagressions visant les particuliers, les entreprises ou plus globalement les pays. Les États-Unis sont l'un des rares pays à détenir un baromètre de la cyberinsécurité[170]. Chaque année en effet, l'*Internet Complaint Center* et le FBI publient les statistiques des plaintes relatives à des fraudes sur le Net[171]. Washington a également pris l'initiative de publier en février 2018 un rapport officiel qui évalue le coût de la cybercriminalité pour l'économie étatsunienne à 109 milliards de dollars pour l'année 2016[172].

Selon l'estimation annuelle publiée par la société de cybersécurité Symantec et réalisée auprès de 157 pays, les trois principaux pays responsables des cyberattaques menées en 2017 sont, par ordre décroissant : la Chine (21%) les États-Unis (11%) et, plus loin derrière, la Fédération de Russie (6%)[173]. L'origine géographique de la cyberattaque ne peut cependant pas toujours être établie avec certitude et ne signifie pas nécessairement l'assentiment des autorités de l'État en question.

Origine géographique des cyberattaques en 2017[174]



D'après cette même étude, les États-Unis ont été, entre 2015 et 2017, les victimes du plus grand nombre de cyberattaques (303), suivis par l'Inde (133), le Japon (87), l'Ukraine (49), la Corée du Sud (45) et la Russie (32)[175]. Il est intéressant de constater que la Chine, considérée comme le pays le plus agressif cybernétiquement, ne fait pas partie des 10 pays les plus attaqués et que la Russie arrive seulement en 7e position du classement.

---

[170] N. Arpagian, *La cybersécurité, Que sais-je ?*, 2018, p. 111.

[171] Le rapport 2017 de l'*Internet Complaint Center* et du FBI est disponible en ligne : https://pdf.ic3.gov/2017_IC3Report.pdf, consulté le 13 décembre 2018.

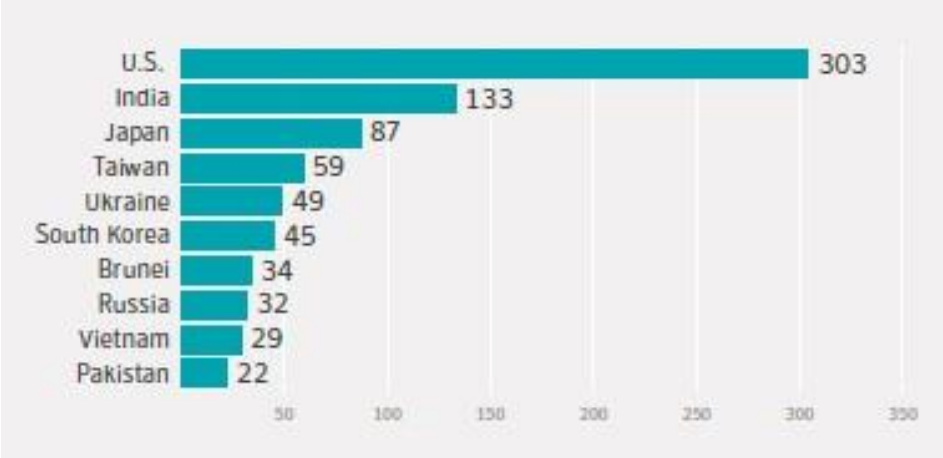
[172] N. Arpagian, *op. cit.*

[173] *Symantec Internet Security Threat Report 2018*, vol. 23, mars 2018, pp. 9, 12.

[174] *Ibid.*

[175] *Symantec Internet Security Threat Report 2018*, vol. 23, mars 2018, p. 32 (https://resource.elq.symantec.com/LP=5840?cid=70138000000rm1eAAA, consulté le 7 décembre 2018).

Top 10 des pays les plus affectés par des cyberattaques entre 2015 et 2017[176]



La France, le Royaume-Uni et l'Allemagne, considérés comme des cyberpuissances européennes à la pointe en matière de cybersécurité, n'échappent pas non plus aux cyberattaques. Ces pays font en effet partie des 10 États dont l'internet des objets (*Internet of Things*-IoT)[177] est le plus vulnérable[178]. Les appareils connectés, dans lesquels un ordinateur et une connexion internet ont été rajoutés, peuvent en effet être victimes de cyberattaques lorsqu'ils ne sont pas correctement protégés.

[176] *Ibid.*

[177] L'Union internationale des télécommunications (UIT) définit l'Internet des objets comme une « infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objects (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution » (UIT, *Série Y : infrastructure mondiale de l'inforamtion, protocole internet et réseaux de prochaine génération. Réseaux de prochaine génération- Cadre général et modèles architecturaux fonctionnels. Présentation générale de l'Internet des objets*, juin 2012, p. 1, https://www.itu.int/rec/T-REC-Y.2060-201206-I/fr, consulté le 18 décembre 2018).

[178] *Ibid.*, p. 80.

Top 10 des pays victimes d'attaques IoT en 2016 et 2017[179]

Rank	Country	2017 Percent	Country	2016 Percent
1	China	21	China	22.2
2	United States	10.6	United States	18.7
3	Brazil	6.9	Vietnam	6
4	Russian Federation	6.4	Russian Federation	5.5
5	India	5.4	Germany	4.2
6	Japan	4.1	Netherlands	3
7	Turkey	4.1	United Kingdom	2.7
8	Argentina	3.7	France	2.6
9	South Korea	3.6	Ukraine	2.6
10	Mexico	3.5	Argentina	2.5

L'Allemagne et le Royaume-Uni font également partie des dix pays les plus touchés par les rançonlogiciels. La quantité de ces cyberattaques est en effet proportionnellement plus élevée dans les pays où le nombre de personnes connectées est le plus important[180]. Par ailleurs, le Royame-Uni, est après l'Irlande, le pays européen où le pourcentage d'attaques par phishing est le plus élevé[181]. Le *phishing* est une technique d'ingénierie sociale qui a pour but de manipuler un individu pour qu'il révèle des informatitions confidentielles sur Internet. Le *phishing* peut permettre à un cybercriminel d'obtenir une fausse identité ou bien de vider un compte bancaire[182]. Enfin, l'Allemagne est le pays européen dont les téléphones mobiles ont été les plus touchés par des logiciels malveillants en 2017[183].

[179] *Symantec Internet Security Threat Report 2018*, *op. cit.*, p. 80.

[180] *Ibid.*, p. 61.

[181] *Ibid.*, p. 69.

[182] A. Desforges et E. Déterville, *op. cit.*, pp. 24-25.

[183] *Symantec Internet Security Threat Report 2018*, *op. cit.*, p. 79.

Pourcentage des cyberattaques au moyen de rançonlogiciels par pays en 2017[184]

Rank	Country	Percent
1	United States	18.2
2	China	12.2
3	Japan	10.7
4	India	8.9
5	Italy	4.1
6	Germany	3.4
7	Brazil	3.1
8	Mexico	2.5
9	United Kingdom	2.3
10	Canada	2.1

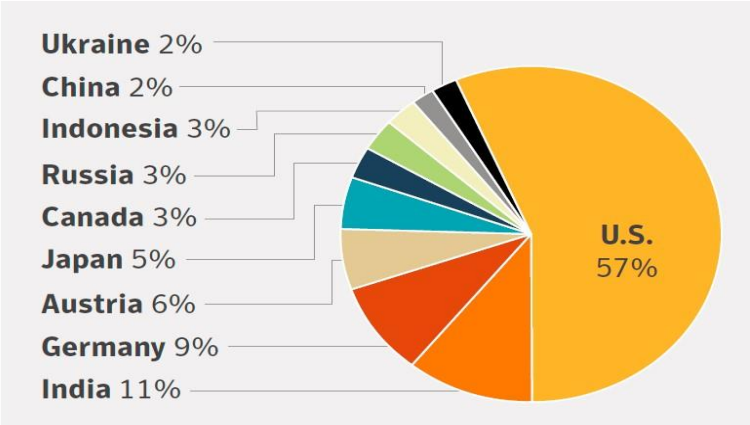
Top 10 des pays victimes de phishing en 2017[185]

Rank	Country	Percent of Email Malware
1	Ireland	32.4
2	Australia	26.7
3	New Zealand	26.3
4	Brazil	23.1
5	Norway	18.0
6	United Kingdom	16.8
7	Mexico	16.4
8	Sweden	16.1
9	Finland	11.5
10	Canada	11.4

[184] *Ibid.*

[185] *Ibid.*, p. 69.

Top 10 des pays victimes de logiciels malveillants sur téléphones portables en 2017 [186]



Selon l'étude réalisée en 2017 par l'institut Ponemon auprès de 254 entreprises issues de sept pays différents (Australie, France, Allemagne, Italie, Japon, Royaume-Uni et États-Unis)[187], les cyberattaques qui préoccupent particulièrement les entreprises, de par leur coût annuel, sont notamment et par ordre décroissant d'impact financier : les incursions par logiciels malveillants ou « maliciels »[188] (*malware* en anglais)[189], les attaques d'ordinateurs qui proviennent de la navigation sur le web (comme la propagation de virus informatiques par exemple), les attaques en déni de service (DOS-*Deny of Service*) destinées à interdire l'accès aux utilisateurs légitimes d'un service Internet, en perturbant le fonctionnement de celui-ci jusqu'à conduire à son blocage[190], le hammeçonnage ou *phishing*, les vols de données sensibles et stratégiques, notamment par des cyberattaques prolongées et ciblées (APT-*Advanced Persistent Threat* menaces persistances avancées) [191], les attaques à but lucratif direct par un recours à des logiciels rançonneurs ou *ransomwares* qui chiffrent les données sur un disque afin qu'elles deviennent incompréhensibles, et exigent le paiement d'une rançon contre la livraison d'une clé permettant le déchiffrement ; et enfin, les cyberattaques par *botnet*, c'est-à-dire au moyen d'un réseau d'ordinateurs infectés par un logiciel malveillant, qui peuvent exercer un contrôle à distance et permettre l'envoi de virus ou des attaques en déni de service à l'insu des véritables propriétaires des ordinateurs[192].

---

[186] *Ibid.*, p. 79.

[187] Ponemon Institute, *2017 Cost of Cybercrime Study. Insights on the Security Investments that make a difference*, p. 5.

[188] *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2008/2004 (INI))*, § AE.

[189] *Symantec Internet Security Threat Report 2018*, *op. cit.* Les logiciels malveillants ont pour but d'infiltrer un ordinateur ou un réseau afin d'entraver son bon fonctionnement ou d'en prendre le contrôle (A. Desforges et E. Déterville, *Lexique sur le cyberespace*, dans dans *Hérodote* 2014/1 (n°152-153), p. 24). Les *malware* peuvent mettre en panne, détourner ou encore détruire des systèmes de contrôle sensibles tels que ceux de centrifugeuses nucléaires, distributeurs de billets, drones de combat ou aiguillage (Thales Belgique, *Les nouvelles tendances de la menace cyber*, 2017).

[190] Ch. Aghroum, *Les mots pour comprendre la cybersécurité. Et profiter sereinement d'Internet*, Paris, 2010, p. 18.

[191] Une « *menace persistante avancée* » « *est une attaque par laquelle une personne non autorisée accède au réseau et passe inaperçue pendant une période prolongée. Une attaque APT vise à voler des données plutôt qu'à porter atteinte au réseau. Sont particulièrement ciblés les secteurs où les informations ont une forte valeur comme la défense nationale, la fabrication et la finance* » (M. Rouse, « Menace persistante avancée » (APT), dans *lemagit.fr*, article consulté le 2 janvier 2018).

[192] https://www.avast.com/fr-fr/c-botnet, consulté le 17 décembre 2018.

Selon Walter Coenraets, directeur de la *Federal Computer Crime Unit* de Belgique, les cybercriminels s'attaquent généralement moins aux systèmes qu'aux utilisateurs. Souvent en effet, les fraudeurs ne visent pas les serveurs extrêmement sécurisés mais bien plutôt les utilisateurs, singulièrement dans les attaques au *ransomware*. Selon lui, la nouvelle règlementation sur la protection des données à caractère personnel de l'Union européenne[193], applicable dans tous les États membres depuis mai 2018[194], « *permet aux citoyens d'obliger les entreprises à renforcer leur sécurité [mais] de ce fait, il devient plus intéressant et plus facile pour les criminels de s'en prendre au consommateur lambda* »[195]. Par ailleurs, d'après Jim Hansen, « *Plus de 90 % des cyberattaques commencent par une tentative de phishing et un salarié qui tombe dans le panneau* » [196]. Le facteur humain joue dès lors un rôle primordial dans la cybersécurité. Sensibiliser l'internaute aux risques liés au numérique constitue un défi majeur.

Cyberattaques les plus coûteuses en 2017[197]

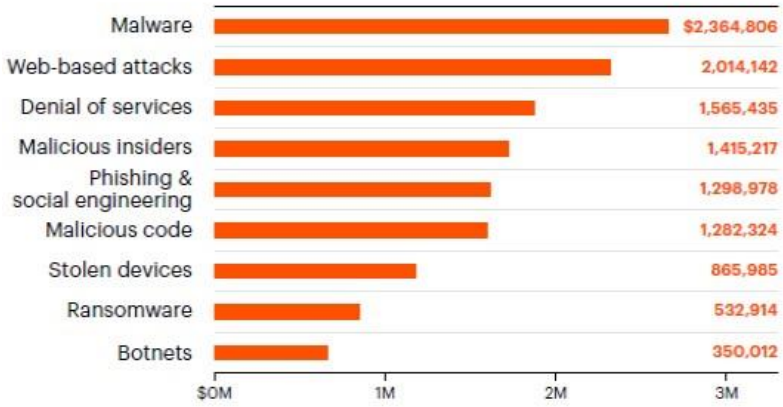


FIGURE 13
Total annualized cyber crime cost for attack types
US$ millions

Legend
Consolidated view
n = 254 separate companies

Les États-Unis et l'Allemagne seraient les deux pays les plus affectés financièrement par la cybercriminalité[198] . Le premier accusant la plus forte hausse de l'impact financier, le second apparaissant comme le mieux armé dans la lutte[199].

---

[193] Le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne vise notamment la protection des données des mineurs et le droit de demander à une entreprise de supprimer des données personnes (E. Roulette, « Protection des données : ce qu'il faut savoir sur le nouveau règlement européen », 23 mai 2018 (https://parismatch.be/actualites/societe/144495/protection-des-donnees-ce-quil-faut-savoir-nouveau-reglement-europeen, consulté le 15 janvier 2019). Le texte du RGPD est disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679).

[194] https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html?locale=fr, consulté le 15 janvier 2019.

[195] S.n., « La Cybersécurité : nous sommes tous concernés », [2017] (https://www.febelfin.be/fr/newsletter360/9/table-ronde-complete, consulté le 15 janvier 2019).

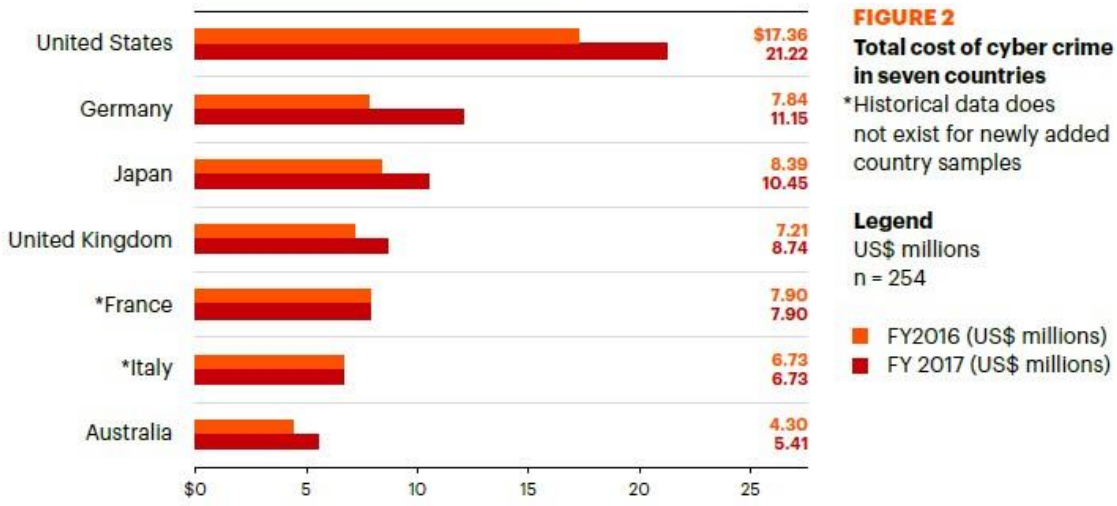
[196] Cl. Weber, « La place de l'homme dans les enjeux de cybersécurité », dans *Stratégique*, n°117, 2018, p. 83.

[197] Ponemon Institute, *2017 Cost of Cybercrime Study. Insights on the Security Investments that make a difference*, p. 27.

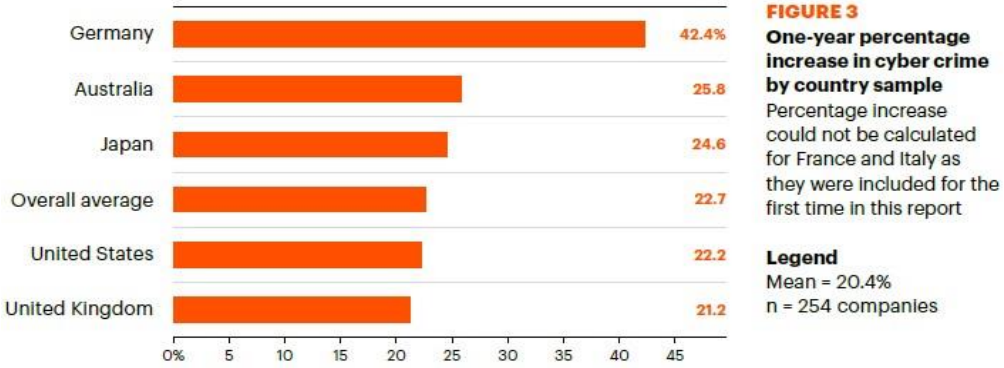
[198] *Ibid.*, p. 13.

[199] *Ibid.*, p. 14.

Coût total de la cybercriminalité par pays en 2016 et 2017[200]



Augmentation en pourcent du coût de la cybercriminalité entre 2016 et 2017[201]



Enfin, tous les pays interrogés s'avèrent vulnérables vis-à-vis des cyberattaques mais sur des critères de sécurité différents[202]. Ainsi par exemple, la France est le pays à qui les attaques provenant du web coûtent proportionnellement le plus cher (20% du coût total annuel lié à la cybercriminalité) tandis que l'Allemagne et l'Australie sont proportionnellement les plus touchés en matière d'attaques par logiciels malveillants (pour chacun des deux pays, 23% du coût total annuel lié à la cybercriminalité)[203].

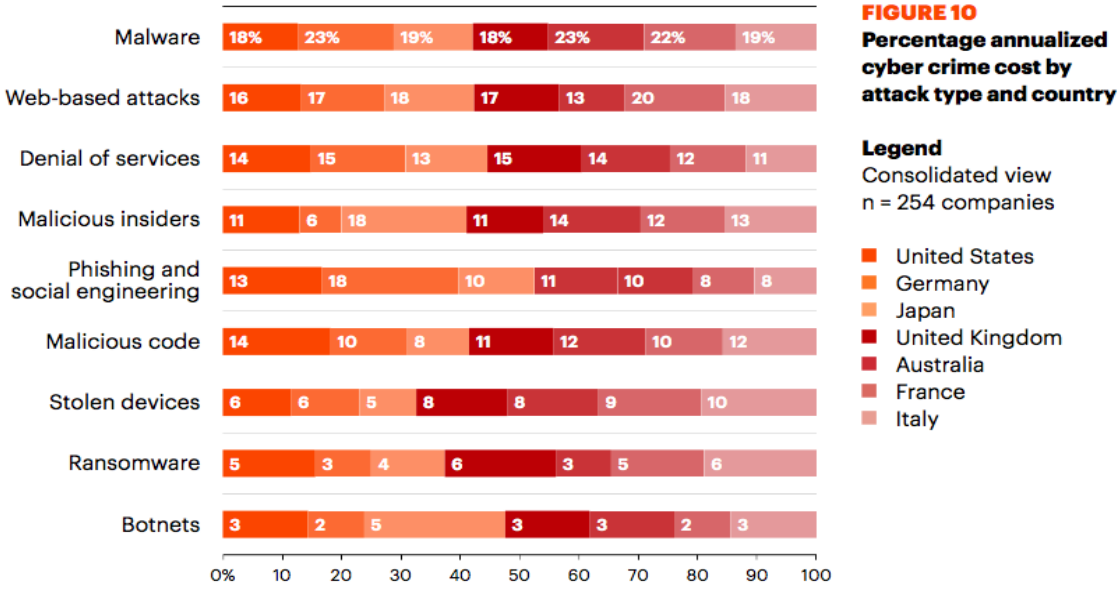
[200] *Ibid.*, p. 13.

[201] Ponemon Institute, *2017 Cost of Cybercrime Study. Insights on the Security Investments that make a difference*, p. 25.

[202] https://www.accenture.com/fr-fr/insight-cost-of-cybercrime-2017, consulté le 17 décembre 2018.

[203] Ponemon Institute, *op. cit.*, p. 25.

Pourcentage du coût de la cybercriminalité par attaque et pays en 2017[204]



Lorsqu'elles sont divulguées, les estimations du coût global des cyberattaques sont généralement incomplètes et peu conformes à la réalité. En effet, les calculs des coûts d'une attaque se limitent habituellement à la partie émergée de l'iceberg et prennent seulement en compte les frais liés aux amendes, dépenses en relations publiques mais également les coûts liés aux actions immédiates à mettre en place pour protéger les individus. Pourtant, lorsque les attaques ont d'autres objectifs que le simple vol des données, les coûts s'avèrent particulièrement difficiles à évaluer. Les conséquences d'une attaque peuvent en effet se répercuter sur des années sous la forme de coûts cachés, dont la plupart sont beaucoup moins facilement mesurables, à savoir l'atteinte portée à l'image du pays ou de l'entreprise, l'interruption d'activité, la perte d'informations confidentielles et/ou stratégiques[205].

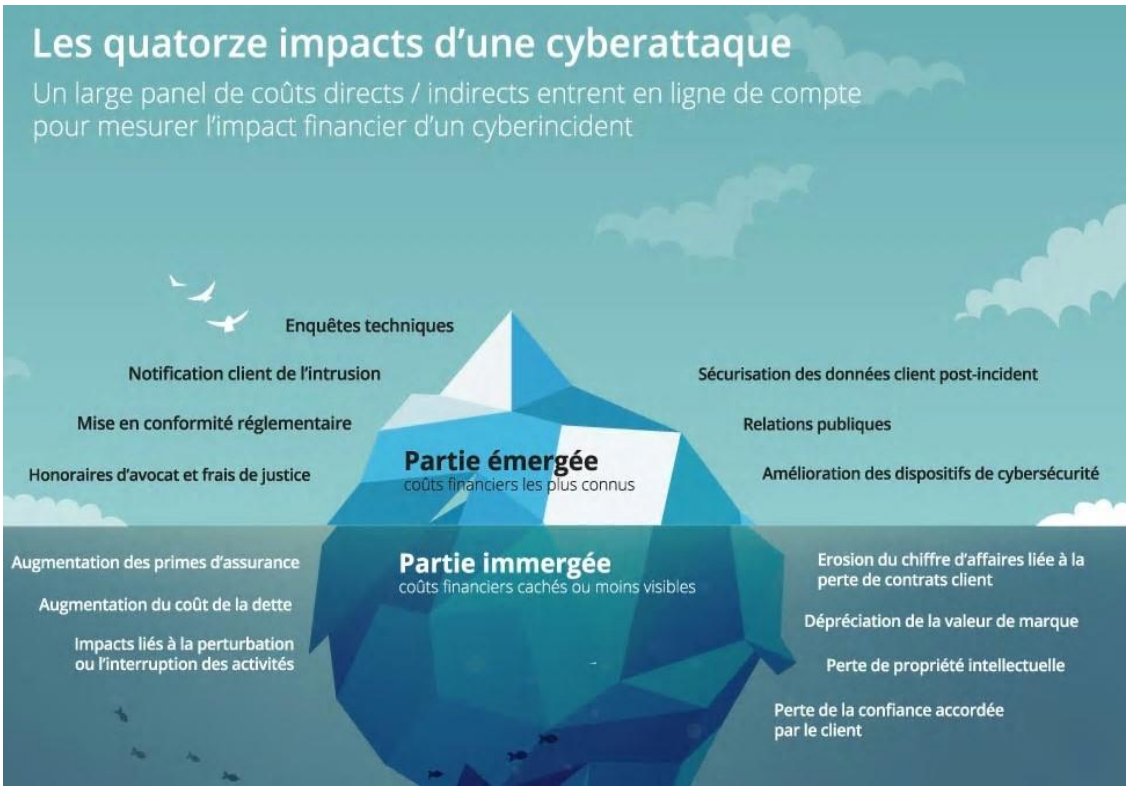
Michael Bittan recense 14 facteurs à prendre en compte pour évaluer de manière exhaustive les conséquences d'une cyberattaque sur une entreprise. Parmi les éléments à considérer, il y a d'une part, la partie émergée de l'iceberg constituée par les coûts directs habituellement associés aux violations de données à caractère personnel. Il s'agit d'autre part de tenir compte de la partie immergée de l'iceberg, à savoir l'ensemble des répercussions beaucoup moins facilement quantifiables et rarement portées à la connaissance du public, comme la dévalorisation financière de la marque, la perte de propriété intellectuelle ou encore l'augmentation du coût des assurances[206].

[204] *Ibid.*

[205] M. Bittan, « Cyberattaques : comment chiffrer les impacts ? Le visible et l'invisible », [2016] (https://www2.deloitte.com/fr/fr/pages/risque-compliance-et-controle-interne/articles/cyberattaques-chiffrer-les-impacts.html#, consulté le 13 décembre 2018).

[206] *Ibid.*

Les quatorze impacts d'une cyberattaque[207]

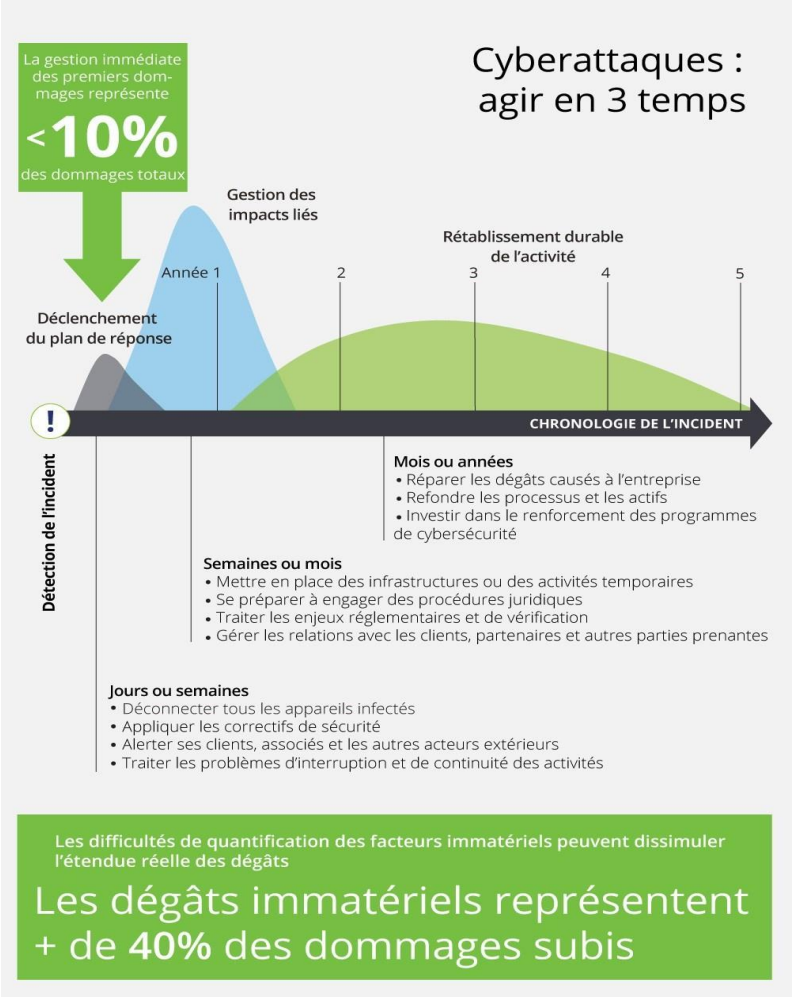


Au-delà de la gestion de ses conséquences immédiates sur les clients de l'entreprise et sur l'entreprise elle-même, une cyberattaque nécessite à plus long terme la mise en place d'actions permettant de réparer les dommages subis. La phase de récupération se déroule en effet en plusieurs étapes : rétablissement de l'activité, augmentation du niveau de cybersécurité, restauration de relations de confiance avec les clients et les parties prenantes, règlement des questions juridiques, décisions d'investissement et changements de stratégie. D'aucuns estiment que les dégâts immatériels représentent plus de 40 % des torts subis tandis que la gestion immédiate des premiers dommages constitue moins de 10 % de la facture totale[208].

[207] *Ibid.*

[208] *Ibid.*

Les répercussions d'une cyberattaque dans la durée[209]



Selon une étude réalisée par Deloitte, 75% des entreprises[210] auraient adopté de nouvelles mesures de cybersécurité depuis les récentes cyberattaques Wannacry et NotPetya[211]. Par ailleurs, au vu de la complexité de la menace cyber, de plus en plus d'entreprises souscrivent à une assurance pour se prémunir des risques. Une telle assurance permet notamment de couvrir une partie des coûts liés aux attaques cybernétiques et de bénéficier de l'assistance d'avocats spécialisés et experts en informatique[212]. Souscrire à une cyberassurance permet également à l'entreprise d'effectuer une évaluation préalable de son niveau de maturité cyber et des différentes vulnérabilités de son système

[209] *Ibid.*

[210] L'étude Deloitte a été réalisée à partir d' un panel de 403 sociétés issues de plus de 150 pays (Deloitte, *Enjeux cyber 2018. L'évolution de la menace Cyber*, Paris, janvier 2018, pp. 22, 25, https://www2.deloitte.com/fr/fr/pages/risque-compliance-et-controle-interne/articles/enjeux-cyber.html, consulté le 19 décembre 2018).

[211] *Ibid.*, p. 6.

[212] https://www.allianz.be/fr/Professionnels/assurance-cyber/assurance-cyber.aspx, consulté le 19 décembre 2018.

d'information[213]. Néanmoins, seules 24 % de ces sociétés bénéficiaient en 2017 d'une cyberassurance[214].

Certains considèrent que les dépenses consacrées aux technologies de gouvernance, de gestion des risques et de conformité « *ne constituent pas une voie rapide vers une sécurité accrue* ».[215] Selon Accenture, ce sont les innovations, comme l' « apprentissage automatique »[216] (en anglais *machine learning*) ou, plus globalement, l'intelligence artificielle (IA), qui génèreraient les meilleurs retours sur investissements, même si ceux-ci restent faibles. En effet, aujourd'hui, un quart seulement (26%) des 254 sociétés interrogées ont développé des technologies de sécurité utilisant l'intelligence artificielle et moins d'un tiers (31%) utilisent l'analytique avancée pour combattre la cybercriminalité[217] Or, si l'on en croit bon nombre de documents marketing et articles de presse, l' « *IA permettrait de remplacer l'expertise humaine, de détecter les incidents de cyber-sécurité de façon beaucoup plus certaine, de répondre automatiquement aux attaques et enfin de s'adapter rapidement à la constante évolution des environnements et à l'augmentation des volumes de données traitées* »[218]. Alain Loute met néanmoins en garde contre le danger d' une « *démocratisation du développement technique* » qui aboutirait à « *renforcer l'emprise de certains acteurs sur ce développement* »[219]. Selon lui, l'autonomisation considérée comme « *inévitable* »[220] des machines « *détourne l'attention d'enjeux de pouvoir qui se posent dès à présent, à savoir que l'autonomisation des robots, le fait de leur déléguer des décisions et de leur laisser choisir par eux-mêmes signifie peut-être la perte du pouvoir de décision de quelques-uns, mais intensifie aussi la concentration de la décision dans les mains de certains (les programmateurs, les propriétaires des robots, etc.)* »[221].

Selon la résolution du Parlement européen du 16 février 2017 qui contient des recommandations à la Commission concernant les règles de droit civil sur la robotique et qui analyse l'émergence des robots, algorithmes intelligents, androïdes et autres formes d'intelligence artificielle, « *il est d'une importance fondamentale pour le législateur d'examiner les conséquences et les effets juridiques et éthiques d'une telle révolution, sans pour autant étouffer l'innovation* »[222]. En effet, si la numérisation

---

[213] Deloitte, *op. cit.*, p. 10.

[214] *Ibid.*, pp. 10, 22, 25.

[215] https://www.accenture.com/fr-fr/insight-cost-of-cybercrime-2017, consulté le 19 décembre 2018.

[216] L'« apprentissage automatique » ou *machine learning* en anglais, est un champ d'étude de l'intelligence artificielle « *qui fait référence au processus par lequel les ordinateurs développent la reconnaissance de schémas ou l'aptitude à apprendre continuellement et à faire des prévisions basées sur des données, puis à faire des ajustements sans avoir été spécifiquement programmés pour le faire* ». (Hewlett Packard Enterprise, « Qu'est-ce que le machine learning ? », 2018, https://www.hpe.com/be/fr/what-is/machine-learning.html, consulté le 20 décembre 2018).

[217] https://www.accenture.com/fr-fr/insight-cost-of-cybercrime-2017, consulté le 19 décembre 2018.

[218] Thales, « L'intelligence artificielle au service de la cyber-sécurité. État de l'art et retour d'expérience », 10 décembre 2018, p. 3 (https://www.thalesgroup.com/fr, consulté le 19 décembre 2018).

[219] A. Loute, « 'Éthique au futur' et pilotage du développement technoscientifique », dans Analyse (une publication action et récherche culturelles ASBL), n°10, 2018, p. 1 (https://arc-culture.be/wp-content/uploads/2018/12/WEB_Analyse_ARC_2018_10_technoscientifique.pdf, consulté le 10 janvier 2019).

[220] *Ibid.*, p. 6.

[221] *Ibid.*, p. 7.

[222] *Résolution du Parlement européen du 16 février 2017 contenant les recommandations à la Commission concernant des règles de droit civil sur la robotique*, Strasbourg, § B (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//FR, consulté le 9 janvier 2019).

de notre société offre de nombreuses opportunités, elle comporte également des risques qui nécessitent attention et initiatives de la part des décideurs politiques. L'apparition d'emplois inédits dans des secteurs qui jusqu'ici n'existaient pas, comme la lutte contre la cybercriminalité ou le *blockchain*[223], et la stimulation d'un nouvel entreprenariat avec de nouveaux produits font partie des avantages liés au développement du numérique. Parmi les défis à relever sur le plan de la cybersécurité figure la nécessité d'améliorer le cryptage des données ainsi que le problème du respect de la vie privée[224]. La question des « big data » fait également partie des enjeux à considérer. Si les données massives, et les algorithmes qui y sont liés, facilitent certaines activités de renseignement, elles ne peuvent effectivement pas remplacer le rôle essentiel des humains dans les questions de sécurité nationale[225].

Critères d'appréciation des cyberpuissances

Selon O. Kempf, « *il est raisonnable de penser qu'il existe une certaine corrélation entre le niveau de puissance classique (économique, technologique et militaire) et le niveau de cyberpuissance* »[226]. Évaluer la cyberpuissance d'un État, c'est-à-dire sa capacité à agir dans l'espace numérique et à assurer sa cybersécurité, n'est pas chose aisée et diffère selon les critères choisis. Ainsi, sept rubriques sont prises en compte par l'OTAN pour juger de la capacité des pays alliés à traiter des problèmes de sécurité dans le cyberespace, à savoir : les moyens de défense des infrastructures et réseaux nationaux , les ressources prévues pour le renforcement des capacitiés de cyberdéfense , les interactions entre les acteurs nationaux , la compréhension des cybermenaces , l'hygiène informatique du pays , les entraînements et exercices en matière de cyberdéfense, et la mise en œuvre des engagements de cyberdéfense aggréés, notamment pour les systèmes nationaux dont l'OTAN est tributaire[227].

L'Union internationale des télécommunications des Nations Unies (*International Telecommunication Union* – ITU) retient quant à elle cinq critères pour apprécier le niveau de cybersécurité d'un pays : l'adéquation du cadre légal pour réagir aux attaques cybernétiques, le degré de compétence technique en matière de prévention et de résilience, notamment par la présence de systèmes de certification[228] de cybersécurité reconnus, le dispositif organisationnel mis en place pour

---

[223] Apparue en 2009, la *blockchain* est une technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe central de contrôle (https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/ et https://www.febelfin.be/fr/newsletter360/9/table-ronde-complete, consultés le 10 janvier 2019).

[224] Sénat de Belgique, *Demande d'établissement d'un rapport d'information relative à la nécessaire collaboration entre l'État fédéral et les entités fédérees en ce qui concerne les retombées, les opportunités, les potentialités et les risques de la 'société intelligente' numérique*, 24 mai 2018, p. 4 (session de 2017-2018 n°6-413/1). Pour plus de détails sur les enjeux relatifs au respect de la vie privée liés à l'internet, les réseaux sociaux et les big data, lire Y. Berbers, M. Hildebrandt et J. Vandewalle (sous la dir.), « Privacy in tijden van internet, sociale netwerken en big data », Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten, *Standpunt* n°49, 2017.

[225] D. Van Puyvelde, « Les enjeux techniques et sécuritaires. Big data, renseignement et sécurité nationale à l'ère cyber », dans S. Taillat, A. Cattaruzza et D. Danet, *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2018, p. 104.

[226] O. Kempf, *Introduction à la cyberstratégie*, Paris, 2012, p. 140.

[227] https://www.nato.int/cps/fr/natohq/official_texts_133177.htm, consulté le 7 novembre 2018.

[228] La certification est « *l'attestation de la robustesse d'un produit [d'un service ou d'un processus des technologies de l'information et de la communication (TIC)], basée sur une analyse de conformité et des tests de pénétration réalisés (…) selon un schéma et un référentiel adaptés aux besoins de sécurité des utilisateurs et tenant compte des évolutions technologiques* » (https://www.ssi.gouv.fr/administration/produits-certifies/, consulté le 1er janvier 2019). Voir aussi https://www.consilium.europa.eu/fr/press/press-releases/2018/06/08/eu-to-create-a-common-

développer, mettre en œuvre et contrôler la bonne application des cyberstratégies, les moyens liés à la recherche et à la formation et enfin, la coopération internationale et nationale en matière de cybersécurité, en ce compris le partenariat entre le secteur public et le secteur privé[229].

Dans sa résolution sur la cyberdéfense de juin 2018, le Parlement européen appelait « *une réponse commune de l'Union* »[230] face aux « *actes de cybermalveillances à visée politique, économique ou de sécurité* »[231] menées, entre autres par la Russie, la Chine et la Corée du Nord[232]. D'aucuns considèrent ces trois pays comme des cyberpuissances particulièrement performantes en matière de cyberguerre.

R. Clarke et R. K. Knake classent les cyberpuissances en fonction de leur capacité défensive, offensive et de leur dépendance dans le domaine cyber. Selon eux, plus les capacités cyber offensives et défensives des pays sont élevées et leur dépendance cybernétique faible[233], plus les États sont considérés comme des puissances dominantes du cyberespace. La Corée du Nord, la Russie et la Chine apparaissent en tête d'un tel classement[234]. Si cette classification apporte un éclairage intéressant, elle est sans doute aussi très dépendante du contexte politique de l'époque de sa publication. Parue en 2010 alors que les États-Unis se heurtent à la Corée du Nord qui vient de bombarder l'île sud-coréenne de Yongpyong[235], elle sert en effet principalement à alimenter une politique de fermeté contre un des « États voyoux »[236]. Par ailleurs, une étude publiée en 2017 et assez comparable à celle de 2010 place cette fois-ci les États-Unis, la Russie et la Chine comme puissances dominantes du cyberespace[237]. Selon R. Koch et M. Golling « *This triangle of cyber offense, cyber defence, and cyber dependence creates a challenging and complex system of interdependencies* »[238]. Et d'ajouter que « *Basically, risk can be seen as a mathematical product of the factors 'probability of occurrence' and impact of the damage'. With respect to cyber, this equation is often extended to a three-factor equation: Cyber Risk= Cyber Offense x Cyber Defence x Cyber Dependence* »[239].

D'autres scientifiques considèrent que la puissance d'un État dans le domaine cyber ne se mesure pas à la seule possession de capacités offensives et défensives mais bien sur « *l'aptitude et la volonté de celui-ci de les employer pleinement. Elle dépend de la détermination à décourager les*

---

cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/, consulté le 1er janvier 2019)

[229] ITU, *Global Cybersecurity Index (GCI) 2017*, pp. 4-5.

[230] *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2008/2004 (INI))*, § AE.

[231] *Ibid.*

[232] *Ibid.*

[233] Un pays dont la dépendance cybernétique est faible est un État qui réussit à « *couper son cyberespace national du cyberespace mondial* » (J. de Lespinois, *op. cit.*, p. 163).

[234] R. Clarke et R. K. Knake, *Cyber war. The next threat to national security and what to do about it*, New York, 2010, p. 148 (cités par J. de Lespinois, « Guerre et paix dans le cyberespace », dans *Stratégique*, n°117, 2018, pp. 163-164).

[235] Ph. Li, «Corée du Nord: l'attaque injustifiable, 15 décembre 2010 », dans *Le Monde* (*https://www.lemonde.fr/idees/article/2010/12/15/coree-du-nord-l-attaque-injustifiable_1453563_3232.html*, consulté le 30 décembre 2018).

[236] J. de Lespinois, *op. cit.*, p. 163.

[237] *Ibid.*, pp. 163-164.

[238] T. Minarik, R. Jakschis, L. Lindström, (Eds), *10th International Conference on Cyber Conflict. Cycon X: Maximising Effects*, Tallinn, 2018, p. 159

[239] *Ibid.*, p. 179.

attaques en augmentant la difficulté, le coût et le risque pour un agresseur. Elle suppose, enfin, que l'État puisse s'appuyer sur une industrie en mesure de relayer ou d'élargir son action »[240].

Top 5 des cyberpuissances dominantes dans un contexte de cyberguerre (classement de 2010)[241]

(Les chiffres de 1 à 9 représentent le potentiel cyber du plus élevé au moins élevé)

Pays	**Cyber offensive**	**Cyber dépendance**	**Cyber défensive**	**Total**	**Total sans tenir compte de la cyber dépendance**
Corée du Nord	2	9	7	18	9
Russie	7	5	4	16	11
Chine	5	4	6	15	11
Iran	4	5	3	12	7
États-Unis	8	2	1	11	9

Selon J. de Lespinois, pour mesurer la cyberpuissance d'un pays en matière de cyberdéfense, il faut également tenir compte de son aptitude à utiliser les moyens des grands acteurs privés qui disposent souvent des ressources financières et techniques les plus importantes[242], du « processus de certification »[243] national mis en place, de la capacité industrielle et du potentiel scientifique des États dans le domaine cybernétique, mais également du degré d'intégration des pays à l'économie mondiale (« degré de connectivité ») [244] ainsi que de la centralité de leurs réseaux informatiques sur la scène internationale[245]. Ainsi, par exemple la relativement faible « connectivité » de la Chine et son manque de centralité fragilisent, selon lui, la puissance numérique de ce pays. Et d'ajouter que si cet État doit utiliser des réseaux américains ou européens pour atteindre ses cibles, il perdra en effet une grande partie de sa puissance offensive dans le cyberespace[246].

[240] *Revue stratégique de cyberdéfense*, 12 février 2018, p. 43 (disponible sur http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/)

[241] Tableau réalisé à partir de l'analyse de R. Clarke et R. K. Knake, *op. cit.* et repris par J. de Lespinois, *op. cit.*, p. 163.

[242] J. de Lespinois, *op. cit.*, pp.158, 168.

[243] *Ibid.*, p. 158.

[244] L'indice de connectivité est la mesure de la capacité et des moyens techniques dont dispose un pays, une ville ou un organisme pour participer à l'économie mondiale. La connectivité permet de comparer le degré d'intégration à l'économie mondiale des métropoles en fonction des flux des biens, de personnes/ de talents, de capitaux et de données. Un indice élevé est associé à une forte performance. En bref, plus une ville, une région ou un pays est connecté, plus il ou elle est prospère (S. n., *Le Grand Montréal, connecté à l'international pour une plus grande richesse collective*, avril 2018, pp. 3, 8).

[245] J. de Lespinois, *op. cit.*, pp. 166-167.

[246] *Ibid.*, p. 167.

Certaines études affirment qu'à l'échelle planétaire, les flux de données[247] numériques génèrent actuellement plus de valeur économique que les flux de biens traditionnels. En effet, depuis la crise économique de 2008, les flux mondiaux de biens et de capitaux stagnent ou déclinent alors que les flux de données numériques continuent à croître de manière exponentielle. Ces flux numériques auraient ainsi été multipliés par 45 entre 2005 et 2014 et devraient encore être multipliés par 9 d'ici à 2021[248]. En outre, les échanges internationaux auraient généré, en 2014, 10% du PIB mondial, dont plus du tiers est attribuable aux flux de données générées à l'échelle de la planète, une forme d'échange qui n'existait pas il y a encore quinze ans[249].

La puissance numérique générée par le degré de connectivité des États serait pour le moment essentiellement l'apanage de quelques « acteurs transnationaux »[250] comme les GAFAM (Google, Amazon, Facebook, Apple et Microsoft) et d'un petit nombre d'États[251]. Selon une étude réalisée par le McKinsey Global Institute (MGI) auprès de 139 États, les flux internationaux restent en effet largement aux mains de quinze pays, repris dans le tableau ci-dessous, qui cumulaient en 2014, 66% du commerce des biens, 62% de la distribution des services, 79% des investissements directs à l'étranger (IDE) et 77% des flux des données.[252]

Index de connectivité MGI des États en 2014 (sur 139 pays)[253]

Connectedness index rank 1–10 11–25 26–50 >50

			Connectedness Index rank				
Rank	Country	Score	Goods	Services	Finance	People	Data
1	Singapore	64.2	1	2	2	12	6
2	Netherlands	54.3	3	3	6	21	1
3	United States	52.7	7	7	3	1	7
4	Germany	51.9	2	4	8	3	2
5	Ireland	45.9	32	1	1	28	9
6	United Kingdom	40.8	13	5	5	6	3
7	China	34.2	4	16	4	82	38
8	France	30.1	11	8	9	7	4
9	Belgium	28.0	5	6	33	33	8
10	Saudi Arabia	22.6	20	28	27	2	53
11	United Arab Emirates	22.2	6	23	17	4	46
12	Switzerland	18.0	12	11	10	17	13
13	Canada	17.3	16	22	11	11	18
14	Russia	16.1	21	25	18	5	25
15	Spain	14.4	25	13	19	14	16

[247] Les flux de données correspondent soit au volume des données acheminées par le Web et des appels internationaux provenant d'un territoire, soit à la valeur des exportations dites « livrables par voie numérique» (S.n., *Le Grand Montréal*, *op. cit.*, p. 7)

[248] J. de Lespinois, *op. cit.*, p. 155.

[249] S.n., *Le Grand Montréal*, *op. cit.*, p. 9.

[250] Selon J. de Lespinois, les acteurs dits multinationaux, c'est-à-dire les entreprises implantées dans plusieurs pays sont devenus des «acteurs transnationaux » du fait de la perte de la puissance des États dans le domaine économique (J. de Lespinois, *op. cit.*, p. 156).

[251] *Ibid.*

[252] *Ibid.*, p. 164.

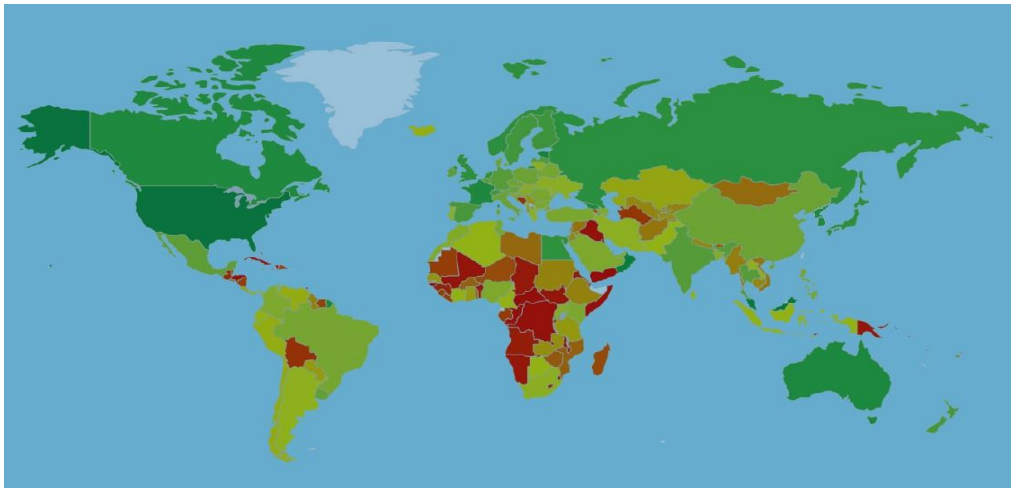
[253] McKinsey Global Institute (MGI), *Digital Globalization: The New Era of Global Flows*, mars 2016, p. 12

Des super cyberpuissances invulnérables?

Si ces différents critères ne sont que des indicateurs de la maturité des politiques de cybersécurité et cyberdéfense, certaines cyberpuissances semblent plus avancées que d'autres en la matière.

États-Unis, leader otanien en matière de cybersécurité

Niveau d'engagement des États en matière de cybersécurité en 2017, selon ITU (de vert foncé : niveau le plus haut à rouge : niveau le plus bas)[254]



Selon l'agence onusienne ITU, la république de Singapour est la nation la plus performante en matière de cybersécurité. Cette cité-État de 5,5 millions d'habitants, qui consacre 3,3% de son PIB à son budget défense[255], aurait en effet des méthodes de protection et de gestion des cyberattaques quasi parfaites[256]. Le pays met en place son premier plan directeur en matière de cybersécurité dès 2005 (*Infocomm Security Masterplan*)[257]. La présence à Singapour de nombreuses entreprises internationales spécialisées dans la cybersécurité représente une source de revenus importante pour la cité-État, estimée à environ 366 millions d'euros. La valeur du marché de la cybersécurité (« *cybersecurity market* ») devrait doubler d'ici à 2020, notamment grâce à un renforcement des infrastructures et services en la matière[258]. Pour continuer à attirer les investissements internationaux, Singapour entend consolider son statut de « hub régional » en assurant un environnement sûr, particulièrement dans le domaine numérique. Singapour représente en effet une des cibles privilégiées des cyberattaques d'Asie et du Pacifique, en raison de son hyper-connectivité et du nombre de multinationales et laboratoires de recherche en lien avec la cybersécurité que la cité-État héberge[259]. Dès 2013, la république a d'ailleurs

[254]ITU, *Global Cybersecurity Index (GCI) 2017*, p. 13 (https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf, consulté le 14 novembre 2018).

[255] https://donnees.banquemondiale.org/indicateur/MS.MIL.XPND.GD.ZS?locations=SG-US-FR-EE-RU, consulté le 9 janvier 2019.

[256] ITU, *Global Cybersecurity Index (GCI) 2017*, pp. 17, 32.

[257] *Singapore's Cybersecurity Strategy*, 2016, p. 5 (https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf).

[258] *Ibid.*, p. 38.

[259] S. n., « Singapour : une place stratégique en Asie du Sud-est », *op. cit.*

entamé un plan appelé « *smart nation* » (nation intelligente) en faveur de la cybersécurité, étalé sur 7 ans et soutenu par un budget d'environ 12 milliards d'euros[260].

Le gouvernement singapourien envisage la problématique numérique d'une manière globale (« *with a comprehensive framework* »[261]) et essaie dès lors d'impliquer l'ensemble de la société dans la cyberdéfense du territoire. Il s'est doté de deux agences spécialisées en la matière : la cyber Security Agency (CAS), placée sous l'autorité directe du Premier ministre et chargée de la lutte contre les cyberattaques d'une part, et la Defence Cyberorganisation, d'autre part. Créée en 2017, celle-ci devrait être constituée à terme de 2600 soldats avec pour vocation de surveiller et défendre les réseaux des forces armées singapouriennes des cyberattaques. Le renforcement des partenariats internationaux, comme l' « ASEAN Cyber Capacity Programme » lancé par Singapour en 2017 afin de renforcer la sécurité des réseaux des pays de l'Asie du Sud-est, fait partie des priorités sécuritaires[262]. En juillet 2018 néanmoins, « *la pire cyberattaque qui ait touché Singapour n'a pu être empêchée* »[263], rapporte *The Straits Times*. Un quart de la population du pays, soit 1,5 million de personnes se sont en effet vu voler leurs données personnelles -certes non médicales- par des hackers, qui ont réussi à infiltrer des ordinateurs de *SingHealth,* le plus important groupe de santé de Singapour[264].

Les États-Unis occupent la deuxième position du classement ITU. Ils se distinguent particulièrement dans le domaine juridique et la recherche[265]. Le pays a très tôt pris en compte la problématique de la cybersécurité. En effet, dès mai 1998, le président Bill Clinton signe le décret présidentiel n°63 qui instaure la protection des infrastructures critiques et vise notamment à mieux protéger leurs systèmes informatiques des cyberattaques. Les attentats du 11 septembre 2001 renforcent l'approche sécuritaire du pays, « *avec l'obsession de ne plus manquer l'information stratégique afin qu'elle soit ensuite exploitée dans le temps* »[266]. Les années qui suivent s'illustrent par la mise en place d'une myriade d'organismes et de programmes spécialisés en cybersécurité[267]. En 2008, le président G.W. Bush approuve la *Presidential National Security directive 54* qui formalise une série de mesures visant à protéger les systèmes d'information gouvernementaux contre les attaques informatiques[268].

Le pays de l'Oncle Sam montre des caractéristiques stratégiques assez nettes : avance technologique aussi bien en termes de logiciels que d'usage de ces technologies ; militarisation précoce du cyberespace ; capacités cybernétiques défensives et offensives ; élaboration d'un système d'alliances contre des adversaires (Iran, Chine) et action résolue dans la guerre de l'information[269]. Depuis 2010, les États-Unis disposent du *US Cyber Command* commandée par le directreur de la NSA (*National Security Agency*), l'agence responsable du renseignement d'origine électromagnétique et de la sécurité

---

[260] *Singapore's Cybersecurity Strategy*, *op. cit.*

[261] *Ibid.*, p. 17

[262] S. n., « Singapour : une place stratégique en Asie du Sud-est », *op. cit*.

[263] S.n., « Les données personnelles de 1,5 million de singapouriens volées lors d'une cyberattaque », 20 juillet 2018, dans *Courrier international.com.*

[264] *Ibid.*

[265] ITU, *Global Cybersecurity Index (GCI) 2017*, pp. 17, 28.

[266] N. Arpagian, *La cybersécurité, Que sais-je ?*, 2010, p.107.

[267] *Ibid.*

[268] S.n., « La cyberdéfense: un enjeu mondial, une priorité nationale », s.d. (http://www.senat.fr/rap/r11-681/r11-68110.html, consulté le 14 janvier 2019).

[269] O. Kempf, *op. cit.*, p. 146. La guerre d'information inclut les opérations sur les systèmes d'information, les opérations électromatgnétiques, les opérations d'influence et le renseignement (S. Taillat, « L'impact numérique sur les relations stratégiques internationales », dans *Stratégique*, n°117, 2018, p. 146).

des systèmes d'information du gouvernement américain. Le *cyber Command* s'est depuis lors structuré de manière à prendre en charge la sécurité et la défense des infrastructures nationales jugées essentielles mais aussi la conduite d'opérations numériques en soutien des opérations militaires[270]. En 2011, le Pentagone publie sa première cyberstratégie dans laquelle le cyberespace apparaît comme un nouveau domaine militaire[271]. D'autres documents stratégiques en matière de cybersécurité sont publiés par la suite, dont la *National Cyber Strategy* en 2018[272].

Selon F. Douzet et S. Taillat, le leadership américain sur le cyberespace illustre néanmoins une double dynamique paradoxale. Elle se traduit en effet par la promotion de normes en faveur de la réduction des risques liés à la conflictualité numérique mais également par une « *militarisation précoce du cyberespace qui engendre de l'instabilité* »[273]. Comme souligné précédemment, les États-Unis ont été en effet, entre 2015 et 2017, les victimes du plus grand nombre de cyberattaques. En 2017, les États-Unis ont investi 19 milliards de dollars dans la cybersécurité, soit une augmentation de 35 % par rapport à l'année précédente[274]. Pour l'année fiscale 2019, le président Trump a d'ailleurs demandé une enveloppe de 15 milliards de dollars (dont 8,5 milliards pour la Défense, soit une augmentation de 4,2% par rapport à 2018) afin de renforcer la sécurité des systèmes d'information de l'État fédéral et de ses agences[275]. Le président américain désire ainsi que son pays « *continue to lead the world in securing a prosperous cyber future* »[276].

Estonie et France, champions européens de la lutte contre les cyberattaques

L'Estonie et la France sont les deux pays de l'UE les mieux classés par l'ITU en matière de cybersécurité. Ils occupent respectivement la 5e et la 8e place sur l'échelle planétaire[277]. Depuis que l'Estonie a pris son indépendance en 1991, ses dirigeants misent sur le numérique pour gagner en efficacité et faire des économies. Le digital est ainsi devenu un réflexe quotidien pour la majeure partie de la population estonienne, à la fois dans les services publics et dans les entreprises privées. Certains préfèrent d'ailleurs utiliser le terme d'« e-Estonie » plutôt que celui d'Estonie. Selon Urve Palo, la ministre estonienne de l'eutrepreneuriat et du numérique, « *En Estonie, à l'exception des mariages, des divorces et des achats immobiliers, toutes les démarches administratives se font en ligne* »[278]. Les Estoniens peuvent en effet, en utilisant une carte d'identité électronique introduite en 2002, et aujourd'hui adoptée par 98% de la population, voter, accéder aux transports en commun, régler leurs

---

[270] S. Taillat, A. Cattaruzza et D. Danet (sous la dir.), *op. cit.*, p. 115.

[271] F. Douzet, « Géopolitique du cyberespace : la cyberstratégie de l'administration Obama », janvier 2018, dans *Bulletin de l'association de géographes français*, p. 145 (https://journals.openedition.org/bagf/1837, consulté le 14 janvier 2019).

[272] https://ccdcoe.org/cyber-security-strategy-documents.html, consulté le 14 janvier 2019.

[273] S. Taillat, A. Cattaruzza et D. Danet (sous la dir.), *op. cit.*,p. 111.

[274] Communication conjointe au Parlement européen et au Conseil. *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017 [JOIN (2017) 450 final], p. 10.

[275] https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf, consulté le 7 novembre 2018.

[276] National Cyber Strategy of the United States of America, septembre 2018, p. II, (https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, consulté le 7 novembre 2018).

[277] ITU, *Global Cybersecurity Index (GCI) 2017*, pp. 36, 59.

[278] A. Cherif et P. Manière, « L'Estonie, royaume du tout-numérique », 5 avril 2018, dans *latribune.fr* (https://www.latribune.fr/technos-medias/internet/l-estonie-royaume-du-tout-numerique-774138.html, consulté le 5 décembre 2018).

impôts, suivre les résultats de leurs enfants à l'école, effectuer une demande de subvention agricole ou encore récupérer des médicaments en pharmacie. L'Estonie autorise également la circulation de véhicules autonomes sur les routes nationales depuis 2017. Á l'horizon 2020, le pays balte prévoit en outre une numérisation de tous les manuels scolaires utilisés dans ses écoles[279].

L'Estonie a par d'ailleurs développé en 2001 la plateforme « X-Road », qui permet à toutes les institutions, administrations et services publiques de stocker et d'échanger leurs données. Sur l'impulsion de Tallinn, qui désire insuffler une nouvelle stratégie digitale au Vieux Continent, la Finlande a accepté le déploiement de la plateforme X-Road sur son territoire. Les deux pays peuvent ainsi échanger, en toute sécurité, une multitude de systèmes d'information publics et privés, comme les informations fiscales des expatriés vivant chez leur voisin[280]. La « *Nordic National CERT Collaboration* », qui regroupe les États baltes et l'Islande, est également un bel exemple de coopération des pays nordiques en matière de cybersécurité[281]. La France a elle aussi signé un accord de coopération numérique avec l'Estonie en mars 2018 afin d'échanger des « *bonnes pratiques d'e-gouvernement, de sécurisation et de développement du numérique* »[282].

Grâce à ce recours au numérique, « *Tout est plus rapide* »[283], affirme Urve Palo. Et d'ajouter, « *Grâce à cela, nous économisons l'équivalent de 2% de PIB par an* »[284]. Vu la faible densité de population et les moyens limités du pays, l'Estonie « *[mise] sur le numérique pour offrir à moindre coût des services de qualité aux citoyens et entreprises* »[285]. Pour donner un coup de fouet à son économie par le tout-numérique, l'Estonie a également créé, en 2014, un statut dit de « e-résident », détenu aujourd'hui par plus de 33 000 personnes. Accessible à tous les étrangers, il permet à chacun de créer son entreprise et de la gérer ensuite à distance, à l'autre bout du monde, tout en bénéficiant localement d'une fiscalité avantageuse. Ce statut est particulièrement prisé par les entrepreneurs britanniques, qui y voient une solution pour rester dans le marché européen après le Brexit[286].

L'Estonie est l'un des premiers pays européens à avoir développé une stratégie nationale de cybersécurité dès 2008, après les cyberattaques de grande ampleur subies l'année précédente[287]. Cette

---

[279] *Ibid. ;* R. Loukil, « L'Estonie, le petit pays qui donne des leçons de numérique au monde entier, dans *Usinenouvelle.com*, 13 juin 2017 (https://www.usinenouvelle.com/article/l-estonie-le-petit-pays-qui-donne-des-lecons-de-numerique-au-monde-entier.N552258, consulté le 10 décembre 2018).

[280] S. Pesic, « L'Estonie : un État 2.0 comme modèle pour l'Europe ? », dans *Lesyeuxdumonde.fr*, 28 juillet 2018 (https://les-yeux-du-monde.fr/actualite/europe/36226-lestonie-un-etat-2-0-comme-modele-pour-leurope, consulté le 5 décembre 2018) ; R. Loukil, *op. cit.*

[281] Cette coopération nordique vise, grâce à une cooperation technique et des exercices communs, à améliorer la prévention, la réaction et le partage d'information en matière de cybersécurité (ITU, *Global Cybersecurity Index (GCI) 2017*, p. 44 ; https://www.msb.se/en/Tools/News/Nordic-cyber-security-exercise-was-conducted-in-Linkoping/, consulté le 6 décembre 2018)

[282] S. Pesic, *op. cit.*

[283] *Ibid.* ; A. Cherif et P. Manière, *op. cit.*

[284] A. Cherif et P. Manière, *op. cit.*

[285] R. Loukil, *op. cit.*

[286] *Ibid.*

[287] En avril 2007, l'Estonie est victime d'une série de cyberattaques sans précédent contre ses sites officiels, ses banques et ses médias, après l'enlèvement dans un jardin public de Tallin d'un mémorial de guerre datant de la période soviétique. Cette cyberattaque de grande ampleur a perturbé pendant plus de deux semaines le fonctionnement institutionnel et médiatique du pays (T. Selhorst, « Russia's Perception Warfare. The Development of Gerasimov's Doctrine in Estonia and Georgia and its Application in Ukraine », dans *Militaire Spectator*, n°4, 2016, pp. 154-155).

cyberstratégie a été actualisée en 2014 et complétée en 2018 par de nouvelles mesures législatives, qui couvrent la sécurité de l'information et la cybersécurité. Parmi celles-ci figure la possibilité d'assurer un niveau minimal d'opérationnalité des infrastructures critiques en cas de cyberattaque[288]. Ainsi, pour éviter une crise comme celle de 2007, l'Estonie a ouvert au Luxembourg, en juillet 2018, une « data embassy », décrite comme une extension du gouvernement estonien sur le cloud. Cette ambassade virtuelle permet en réalité à l'Etat de disposer de serveurs en dehors de son territoire pour sauvegarder une copie de ses données. L'objectif consiste à assurer la continuité des services publics en cas de crise, qu'il s'agisse d'une cyberattaque, d'une catastrophe naturelle ou d'une panne d'électricité. L'élément déclencheur de ce projet a été l'annexion de la Crimée par la Russie en 2014. L'Estonie redoute en effet de subir le même sort que la république et désire dès lors se prémunir des velléités potentielles de Moscou la concernant[289]. L'idée serait de développer, dans le futur, au moins une ambassade cloud par continent[290]. Enfin, le fait que le Centre d'excellence de la cybersécurité de l'OTAN soit basé en Estonie témoigne de la volonté de ce pays de renforcer sa résilience en matière de cyberdéfense. En outre, s'il n'existe pas de partenariat public-privé formalisé, des entités du public collaborent dans les faits avec des organisations du privé[291]. Le budget annuel consacré par l'Estonie à la cybersécurité est estimé à 60 millions d'euros[292]. Ce pays à la pointe du numérique a néanmoins dû suspendre, en novembre 2017, les certificats de sécurité d'environ 760 000 cartes d'identité électroniques nationales munies d'une puce défectueuse (soit près de 60% des cartes d'identité estoniennes), afin de réduire le risque de vols d'identité[293].

La cybersécurité et la cyberdéfense sont devenues depuis plusieurs années une priorité pour les autorités françaises[294]. Les cyberattaques sont ainsi la troisième menace prise en compte dans la stratégie de défense et de sécurité nationale de la république, après les agressions par un autre État contre le territoire national et les attaques terroristes[295]. Le Livre blanc sur la Défense et la Sécurité nationale de 2013 (LBDSN 2013) préconise que la France développe « *sa posture sur la base d'une organisation de*

---

[288] https://www.riigiteataja.ee/en/eli/523052018003/consolide, consulté le 5 décembre 2018; https://ccdcoe.org/cyber-security-strategy-documents.html, consulté le 5 décembre 2018.

[289] A. Cherif et P. Manière, *op. cit.*

[290] R. Loukil, *op. cit.*

[291] ITU, *Global Cybersecurity Index (GCI) 2017*, pp. 36-37 ; BSA, Tableau de bord de la cybersécurité dans l'UE. Vers un cyberespace européen sécurisé, janvier 2015 (http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_fr.pdf, consulté le 21 novembre 2018

[292] R. Loukil, *op. cit.* L'Estonie consacre par ailleurs 2% de son PIB aux dépenses militaires (https://donnees.banquemondiale.org/indicateur/MS.MIL.XPND.GD.ZS?locations=SG-US-FR-EE-RU, consulté le 9 janvier 2019).

[293] https://www.latribune.fr/economie/international/piratage-d-identite-l-estonie-suspend-ses-cartes-id-electroniques-suite-a-la-decouverte-d-une-faille-756647.html, consulté le 9 janvier 2019.

[294] La France a initié le développement de sa cybersécurité depuis la publication du Livre Blanc de 2008 et continue d'amplifier cet effort comme l'ont montré le Livre blanc sur la Défense et la Sécurité nationale de 2013 (LBDSN 2013), les lois de programmation militaire de 2013 (LPM 2013) et 2018 (LPM 2018) mais également la publication, en 2015, d'une version révisée de la « stratégie de cybersécurité nationale » (*Revue stratégique de cyberdéfense*, 12 février 2018, pp. 43-44 (http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf, consulté le 21 novembre 2018) ; N. Arpagian, *La cybersécurité, Que sais-je ?*, 2010, p. 103 ; Loi n°2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense (*https://www.defense.gouv.fr/content/download/.../joe_20180714_0161_0001.pdf*, consulté le 22 novembre 2018).

[295] Stratégie nationale [de la République française] pour la sécurité du numérique, 2015, p. 14 ; *Livre blanc sur la Défense et la Sécurité nationale de 2013*, Paris, 2013, p. 47.

cyberdéfense étroitement intégrée aux forces, disposant de capacités défensives et offensives pour préparer ou accompagner les opérations militaires »[296]. Les autorités françaises désirent néanmoins disposer d'une certaine souveraineté numérique, nécessaire à la préservation de la souveraineté nationale, en conservant une capacité autonome d'appréciation, de décision et d'action[297]. La *Stratégie internationale de la France pour le numérique*, publiée en 2017, préconise également une autonomie stratégique numérique européenne[298]. Présenté en février 2014, le « Pacte Défense Cyber » du ministère de la Défense français prévoit une allocation d'environ un milliard d'euros réparti sur une période de 5 ans (2014-2019), soit un budget annuel d'environ 165 millions d'euros consacré à la cyberdéfense française. La moitié de ce budget sera attribué aux besoins capacitaires du ministère (ressources humaines, moyens techniques) et l'autre moitié au secteur de la recherche et de l'innovation, permettant ainsi au secteur privé de bénéficier de subventions finançant les projets d'innovation technologique dans le domaine de la sécurité des systèmes d'information[299].

La France, qui consacre 2,2% de son PIB aux dépenses militaires[300], a entrepris le virage cyber en se dotant d'un dispositif de sécurité globalement adapté aux enjeux de la cybersécurité : mise en place, en 2009, de l'agence nationale de la sécurité des systèmes d'information (ANSSI), désignation, en 2011, d'un officier général de cyberdéfense à l'état-major des armées et publication, la même année, de sa première cyberstratégie nationale[301], ou encore, création en 2017, d'un commandement de cyberdéfense (ComCyber) au ministère des Armées[302]. Il est prévu que ce commandement ait autorité sur 3200 personnes, soit 2600 combattants numériques et 600 experts de la direction générale de l'armement-DGA) participant à la mission cyber d'ici à 2019[303]. Comme l'annonçait Jean-Yves Le Drian en 2016, la France estime en effet « *nécessaire de créer une nouvelle composante au sein des armées pour asseoir [sa] souveraineté et son indépendance nationales, et rester ainsi maîtr[e] de [son] destin* »[304]. La loi de programmation militaire de 2013 (LPM de 2013) prévoit ainsi de multiplier par trois les crédits [de la Défense] dédiés au développement et à l'acquisition de nouvelles solutions de

---

[296] *Ibid.*, p. 94.

[297] *Stratégie nationale [de la République française] pour la sécurité du numérique*, 2015, p. 7 ; *Revue stratégique de cyberdéfense*, 12 février 2018, p. 93.

[298] Selon *La Stratégie internationale de la France pour le numérique*, *« Ensemble, les États membres disposent de la masse critique et des atouts nécessaires pour porter une conception du numérique qui soit fidèle aux valeurs européennes et qui assure un équilibre satisfaisant entre le développement économique, les nouvelles interactions sociales, le respect des droits et libertés fondamentaux et la sécurité, permettant à l'Union d'atteindre une autonomie stratégique en la matière »* (*Stratégie internationale de la France pour le numérique*, 2017, p. 5, https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf, consulté le 23 novembre 2018.

[299] Ministère de la Défense de la république française, *Pacte Défense Cyber, 50 mesures pour changer d'échelle*, p. 5 ; V. Joubert, *op. cit.*

[300] https://donnees.banquemondiale.org/indicateur/MS.MIL.XPND.GD.ZS?locations=SG-US-FR-EE-RU, consulté le 9 janvier 2019.

[301] https://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/, consulté le 14 janvier 2019.

[302] R. Danesi et L. Harribey, *Rapport d'information fait au nom de la commission des affaires européennes sur la cybersécurité dans l'Union européenne*, n°458, avril 2018, pp. 11-12 ; O. Kempf, *Introduction à la cyberstratégie*, Paris, 2012, p. 151.

[303] *Revue stratégique de cyberdéfense*, 12 février 2018, p. 44 ; M. Cabirol, « Cyberdéfense, une guerre clandestine permanente ? », dans *Latribune.fr*, 30 mai 2017.

[304] J. Guisnel, « Le Drian muscle la cyberdéfense », dans *Lepoint.fr*, 13 décembre 2016.

cybersécurité, soit un budget de 440 millions d'euros sur la période 2014-2019[305]. Le général de Villiers semble cependant opposé au concept de « 4e armée » pour définir la cyberdéfense. Il estime en effet que « *[La France a] trois armées et ce serait une erreur de vouloir créer (…) une quatrième armée de la cyberdéfense* »[306]. Mieux vaut parler, selon lui, d'un « *milieu de combat (au même titre que la terre, l'air et la mer), mais un milieu totalement transverse* »[307]. Et d'ajouter, « *nous ne serons efficaces dans cet espace qu'à condition de mener des actions collectives de manière transverse* »[308]. Enfin, il convient de mentionner la création d'un poste d'ambassadeur pour le numérique en novembre 2017. Il a notamment pour mission le suivi des négociations internationales sur la cybersécurité, la gouvernance des réseaux mais également la liberté d'expression sur internet[309]. Depuis janvier 2019, l'armée française dispose d'une doctrine de lutte informatique offensive afin de muscler la posture de la France face à la multiplication des menaces dans le cyberespace. Le 18 janvier 2019, la ministre française des Armées, Florence Parly a ainsi déclaré qu' « *En cas d'attaque cyber [des forces française], [la France se réserve] le droit de riposter mais [sera] aussi [prête] à employer en opérations extérieures l'arme cyber à des fins offensives, isolément ou en appui de [ses] moyens conventionnels, pour en multiplier les effets dans le plus strict respect des normes du droit international public*»[310]. La récente Loi de programmation militaire (LPM) 2019-2025 de la France prévoit le recrutement de 1000 cybercombattants supplémentaires pour atteindre un effectif de 4000 personnes d'ici sept ans. Par ailleurs, quelque 1,6 milliard d'euros seront investis dans le cyber dans les 6 prochaines années[311].

Le cadre légal français pour réagir aux attaques cybernétiques est particulièrement développé. Ainsi la loi de programmation militaire de 2013 prévoit notamment la notification obligatoire à l'ANSSI des incidents de sécurité informatique et la possibilité pour cette agence d'imposer aux opérateurs d'importance vitale (OIV) de respecter une vingtaine de règles de cybersécurité[312]. Enfin, la France investit beaucoup dans la recherche et la formation relatives à la cybersécurité. Ainsi, l'ANSSI a lancé en 2013 le projet CyberEdu, qui a pour objectif d'introduire les notions de cybersécurité dans l'ensemble des formations en informatique de France[313]. En 2014, le Pôle d'Excellence Bretagne a été mis en place afin de stimuler le développement de l'offre de formation cyber (plus d'une centaine recensée[314]), de la recherche académique cyber et d'une base industrielle et technologique de cybersécurité, avec une attention particulière portée aux petites ou moyennes entreprises et/ou industries (PME-PMI) innovantes[315]. Outre l'action de l'État, les acteurs privés jouent également un rôle important dans le

---

[305] M. Cabirol, *op. cit.*

[306] *Ibid.*

[307] *Ibid.*

[308] *Ibid.*

[309] R. Danesi et L. Harribey, *Rapport d'information fait au nom de la commission des affaires européennes sur la cybersécurité dans l'Union européenne*, n°458, avril 2018, p. 12.

[310] S. n., « Cyberdéfense: Paris montre les crocs», 18 janvier 2019 (https://www.dhnet.be/dernieres-depeches/afp/cyberdefense-paris-montre-les-crocs-5c41f184d8ad5878f01c4c0a, consulté le 19 janvier 2019).

[311] *Ibid.*

[312] https://www.ssi.gouv.fr/entreprise/protection-des-oiv/la-cybersecurite-en-action/, consulté le 22 novembre 2018 ; la liste de la vingtaine de règles de cybersécurité est disponible à l'adresse suivante, consultée le 22 novembre 2018 : https://www.ssi.gouv.fr/entreprise/protection-des-oiv/les-regles-de-securite/

[313] https://www.ssi.gouv.fr/entreprise/formations/cyberedu/, consulté le 22 novembre 2018.

[314] Les questions de cyberdéfense ont par ailleurs été intégrées dans tous les cours d'éducation et de formation militaires (https://www.pole-excellence-cyber.org/formations/toutes-les-formations-des-membres-du-pole-dexcellence-cyber/?by_domain=41, consulté le 23 novembre 2018).

[315] https://www.pole-excellence-cyber.org/presentation-du-pole/, consulté le 23 novembre 2018.

dispositif de sécurité informatique français. La France dispose en effet de grands groupes (Thalès, Orange et Atos), acteurs européens et mondiaux, et d'un réseau d'entreprises plus petites, mais souvent innovantes[316].

Le Royaume-Uni et l'Allemagne occupent respectivement les 4e et 11e place du classement ITU relatif à la cybersécurité des pays de l'UE[317]. Les deux pays disposent d'une cyberstratégie depuis le début des années 2010[318] mais également d'un système de partenariat public-privé bien développé, avec une forte participation active du privé. Cette approche collaborative s'appuie sur les stratégies de cybersécurité en place dans ces deux pays[319]. Ainsi par exemple, l'Allemagne développe depuis 2005 l'« UP KRITIS » (*Umsetzungsplan Kritische Infrastructuren),* plan de coopération entre les secteurs privés et publiques pour assurer la cybersécurité des infrastructures nationales[320]. L'arsenal juridique de ce pays témoigne par ailleurs de l'intérêt apporté à cette coopération[321]. Le code pénal allemand prévoit 10 ans de prison pour des actions de sabotage informatique. Berlin s'est également doté, en août 2009, d'une loi destinée à « renforcer la sécurité de l'information du gouvernement », afin de consolider les moyens et les effectifs de son Office fédéral de sécurité des systèmes d'informations (*Bundesamt für Sicherheit in der Informationstechnik*-BSI), agence nationale créée en 1991 afin de coordonner les activités de cybersécurité[322].

Le Royaume-Uni est également à la pointe dans le partenariat public-privé[323]. Ainsi par exemple, le *Centre for the Protection of National Infrastructure* (CPNI) organise des échanges d'information par secteur et couvre 14 secteurs[324]. Les budgets alloués par les deux pays à la cybersécurité sont en croissance constante. Ainsi, le Royaume-Uni prévoit d'investir un budget de 1,11 milliards d'euros (1,9 milliards de Livres Sterling) entre 2016 et 2021 afin de mettre en œuvre sa stratégie nationale de cybersécurité, contre près de 724 millions d'euros (650 millions de Livres Sterling) entre 2011 et 2015[325]. Si le budget de cyberdéfense de l'Allemagne n'est pas directement connu, il est suffisant pour permetre à Berlin de disposer de capacités cyber-offensives. Le BSI dispose par ailleurs d'un budget annuel d'environ 80 millions d'euros[326]. Enfin, le gouvernement fédéral a annoncé sa décision de fonder en 2019 une agence pour l'innovation dans la cybersécurité (*Agentur für Innovation in der Cybersicherheit*). L'objectif de cette agence est de financer et promouvoir des activités de recherche et

---

316 R. Danesi et L. Harribey*, Rapport d'information fait au nom de la commission des affaires européennes sur la cybersécurité dans l'Union européenne*, n°458, avril 2018, p. 13.

317 ITU, *Global Cybersecurity Index (GCI) 2017*, p. 56.

318 Les documents sont téléchargeables sur https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-for-germany et https://ccdcoe.org/cyber-security-strategy-documents.html.

319 BSA, *Tableau de bord de la cybersécurité dans l'UE. Vers un cyberespace européen sécurisé*, janvier 2015, pp.11, 16 ;

320 UP KRITIS, Public-Private PArtnership Criticas Infrastructure Protection, Bonn, 2014, p. 6 (http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.pdf?__blob=publicationFile, consulté le 6 décembre 2018).

321 BSA, *op. cit.*, p. 11.

322 N. Arpagian, *La cybersécurité, Que sais-je ?* 2010, p. 116; V. Joubert, *op. cit.*

323 HM Government, *National Cyber Security Strategy 2016-2021*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, consulté le 6 décembre 2018.

324 BSA, *op. cit.*, p. 16.

325 HM Government, *National Cyber Security Strategy 2016-2021*, p. 6; V. Joubert, *op. cit.*

326 V. Joubert, *op. cit.*

de développement dans la cybersécurité qui comportent un haut potentiel d'innovation afin de renforcer la sécurité de l'Allemagne. Le budget prévu pour ce projet s'élève, sur une période de 5 ans, à près de 200 millions d'euros[327].

Après avoir tenté de mieux comprendre l'impact des piratages informatiques sur la mise en place d'une cyberstratégie euro-atlantique, l'étude, dans sa seconde partie, visera à analyser celle qui a été développée par la Belgique pour garantir la cybersécurité du pays et participer au projet euro-atlantique.

[327] Ph. Régniez, « Création d'une agence allemande pour l'innovation dans la cyber-sécurité », 5 septembre 2018 (https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-scientifique/veille-scientifique-et-technologique/allemagne/article/creation-d-une-agence-allemande-pour-l-innovation-dans-la-cyber-securite, consulté le 10 décembre 2018).

Partie 2 : La cyberstratégie de la Belgique : défis nationaux et internationaux

Jean-Claude Juncker déclarait en septembre 2017 : « *les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars. (…) Les cyberattaques ne connaissent pas de frontières, elles n'épargnent personne* »[328]. La numérisation de la société accroît en effet sa vulnérabilité à la menace, au point de créer un risque systémique pour les États, les sociétés et les économies[329]. La Belgique n'échappe pas à ce péril. Selon l'étude MGI de 2016, la Belgique occupe la 9e position sur 139 pays en matière de connectivité[330]. En 2017, environ 88% de la population belge avait accès à l'internet contre 29% en l'an 2000[331]. Actuellement, le pourcentage d'internautes en Belgique équivaut à celui de l'Estonie mais est plus élevé que celui des États-Unis[332]. Á l'échelle planétaire, notre pays se trouve d'ailleurs en tête du processus d'adoption du nouveau protocole Internet IPv6, qui permet d'attribuer une adresse IP unique à chaque utilisateur, ce qui présente des avantages évidents en matière de répression et d'enquêtes sur la cybersécurité[333]. En 2017, la Belgique enregistrait le plus fort taux d'adoption du protocole IPv6 au monde, grâce notamment à une coopération entre le secteur public et le secteur privé[334].

Les réseaux informatiques civils et militaires de la Belgique sont en permanence confrontés à des incidents cyber[335]. La *Computer Emergency and Reponse Team* belge (CERT.be) recensait déjà en 2016 une moyenne mensuelle de 1300 cyberinfractions sur le territoire belge[336]. Les exemples ne manquent pas. Ainsi, depuis 2007, l'e-banking de notre pays fait l'objet de cyberattaques régulières[337].

---

[328] R. Danesi et L. Harribey, *Rapport d'information sur la cybersécurité dans l'Union européenne*, n° 458, Sénat, 20 avril 2018, p. 5.

[329] *Ibid.*, p. 8.

[330] McKinsey Global Institute (MGI), *Digital Globalization: The New Era of Global Flows*, mars 2016, p. 12.

[331] The World Bank Group, *Individuals using the Internet (% of population)*, 2017, https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BE, consulté le 14 janvier 2019).

[332] En 2000, 43% de la population des États-Unis avaient accès à l'internet contre 76% en 2016 et 86,5% la même année en Belgique (https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BE-US-EE, consulté le 14 janvier 2019).

[333]Communication conjointe au Parlement européen et au Conseil. *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017 [JOIN (2017) 450 final], p.16 ; https://www.akamai.com/uk/en/about/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp, consulté le 10 octobre 2018 ; L'IPv6 (*Internet Protocol version 6*) constitue l'un des processus standardisés de transfert de paquets de données sur les réseaux informatiques. (https://www.ionos.fr/digitalguide/serveur/know-how/quels-sont-les-avantages-de-ipv6/, consulté le 21 janvier 2019). Les parties prenantes de ce protocole ont envisagé de « *limiter l'utilisation d'une adresse IP à un maximum de 16 utilisateurs dans le cadre d'une mesure volontaire d'autorégulation, ce qui a encouragé la transition vers l'IPv6* » (Communication conjointe au Parlement européen et au Conseil. *Résilience, op. cit.*).

[334] *Ibid.*

[335] Thales Belgique, *Les nouvelles tendances de la menace cyber*, 2017.

[336] *Compte rendu integral avec compte rendu analytique traduit des interventions de la Commission de l'Intérieur, des Affaires générales et de la Fonction publique*, Chambre des représentants de Belgique, p. 6 (CRIV 54 COM 668).

[337] *Cyber Security Strategy [of] Belgium*, 23 novembre 2012, p. 4.

En 2011 déjà, l'opérateur de téléphonie Belgacom est victime d'un piratage informatique important[338]. En 2014, l'ordinateur du premier ministre belge de l'époque, Élio Di Rupo, est également piraté[339]. L'année suivante Proximus fait face à une cyberattaque destinée à voler des données sensibles de l'entreprise, ce que d'aucuns attribuent aux Britanniques[340]. En 2016, une tentative d'intrusion sur le réseau de l'aéroport de Zaventem échoue[341]. Au printemps 2017, les attaques Wannacry et Petya/notPetya n'épargnent pas non plus la Belgique[342]. Enfin, le Centre pour la cybersécurité Belgique (CCB) vient d'ouvrir une enquête afin d'émettre un avis détaillé concernant la filiale belge de Huawei, soupçonnée de cyberespionnage. L'entreprise chinoise fournit déjà depuis dix ans les stations de base des réseaux de Proximus et Orange Belgium. En 2016 et 2017, les services publics fédéraux de la Justice et de la Sécurité sociale ont par ailleurs acheté 580 smartphones à Huawei. En fonction des résultats de l'enquête, la Belgique pourrait interdire toute activité à ce fournisseur sur son territoire[343]. Enfin, une étude menée par PwC (*PricewaterhouseCoopers*) révèle que 53% des entreprises belges ont été confrontées à la cybercriminalité en 2017[344]. Ce chiffre est sans doute à relativiser, au vu du nombre peu important de compagnies qui ont bien voulu collaborer à l'enquête[345].

Selon M. De Bruycker, directeur du Centre pour la Cybersécurité Belgique, le défi actuel auquel est confrontée la cybsersécurité est l'ajustement des moyens juridiques, organisationnels et techniques existants pour une réponse appropriée à cette nouvelle menace, dont l'évolution est de plus en plus rapide[346]. La vitesse du développement technologique est en effet telle qu'elle ne permet pas la protection de nombreux systèmes et facilite dès lors leur prise de contrôle par des criminels[347]. Selon Jan De Blauwe, président de Secursys, comité de Febelfin (Fédération belge du secteur financier) chargé de la cybersécurité au sein des banques, un des défis pour la Belgique consiste à savoir associer ses technologies financières de pointe, en matière d'identité numérique, de cryptage ou de réseau interbancaire SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) par exemple,

---

[338] J.-P. Stroobants, « Belgique : l'opérateur de téléphonie Belgacom victime d'un piratage informatique, 17 septembre 2013 », dans *le monde.fr*, consulté le 28 septembre 2018.

[339] *Question n° 1398 de monsieur le député Brecht Vermeulen du 24 janvier 2018 au ministre de la Défense, chargé de la Fonction publique*, La Chambre des représentants de Belgique, p. 356.

[340] Thales Belgique, *Les nouvelles tendances de la menace cyber*, 2017 ; Ch. Lamfalussy, « Les pirates russes ont frappé à l'Otan et chez Proximus : un espionnage 'tous azimuts' », dans *lalibre.be*, consulté le 28 septembre 2018 ; S.n., « Huawei passée au crible par la Belgique», dans *l'Écho,* 7 décembre 2018, *L'Écho* https://www.lecho.be/tech-media/telecom/huawei-passee-au-crible-par-la-belgique/10076807.html, consulté le 14 décembre 2018).

[341] Thales Belgique, *Les nouvelles tendances de la menace cyber*, 2017.

[342] S.n., « Ransomware 'Wannacry' : l'impact reste limité en Belgique », 15 mai 2017, dans *rtbf.be*, consulté le 28 septembre 2018 ; https://www.cert.be/fr/docs/cyberattaque-petyanotpetya-ransomware.html, consulté le 28 septembre 2018.

[343] S.n., « Huawei passée au crible par la Belgique», *op. cit.*

[344] https://www.safeonweb.be/fr/actualite/testez-la-solidite-de-votre-entreprise-face-aux-cyberattaques, consulté le 16 janvier 2019.

[345] L. Paoli, J. Visschers, C. Verstraete et E. van Hellemont, *The Impact of Cybercrime on Belgian Businesses*, septembre 2017 , p. 24 (http://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwiDk9aq2fLfAhXjxIsKHYSBBagQFjABegQICBAC&url=http%3A%2F%2Fwww.belspo.be%2Fbelspo%2Ffedra%2FBR%2FBCC_ImpactCybercrimeBelgianBusinesses.pdf&usg=AOvVaw1aQq3OtKIchELJCndYTJbj, consulté le 16 janvier 2019).

[346] M. De Bruycker, « Cyber Defence », dans *Revue Militaire Belge*, n°1, décembre 2010, pp. 35, 38.

[347] *Cyber Security Strategy [of] Belgium*, 23 novembre 2012, p. 4.

à une série de technologies innovantes en matière de cybersécurité, « *de sorte à les rendre utiles pour l'utilisateur final et à le convaincre de leur pertinence et leur sûreté* »[348]. Il estime nécessaire que soit mise en place « *une norme de qualité pour les fournisseurs de technologies, de préférence au niveau européen* »[349].

En décembre 2018, la commission des Affaires institutionnelles du Sénat a été chargée de rédiger un rapport d'information relatif à *« la manière dont l'État fédéral et les entités fédérées doivent collaborer afin de tirer profit du potentiel et des opportunités énormes offertes par [la] 'société intelligente' tout en minimisant le plus possible les risques associés* »[350]. Selon les sénateurs, la cybersécurité fait partie des « *énorme[s] défi[s]* » [351] à relever dans notre société où « *la numérisation s'intensifie et l'utilisation de l'intelligence artificielle (IA), ainsi que d'appareils, de technologies et de processus 'intelligents' s'immisce dans tous les domaines de notre vie quotidienne* »[352] (sic).

Dans sa dernière évaluation du niveau de cybersécurité des États, l'ITU place la Belgique en 27e position, sur 165 pays pris en compte et en 10e position sur les 28 États membres de l'Union européenne[353]. Selon cette étude, si la coopération nationale et internationale mais également la capacité de résilience et de prévention constituent les points forts de notre pays, des progrès peuvent encore être réalisés dans la formation et les partenariats entre les secteurs privé et public[354]. D'après J. De Blauwe, la Belgique connaît une « *maturité appréciable en matière de cybersécurité* »[355]. Et d'ajouter que « *Nous avons connu une vague de fraude entre 2012 et 2014 -avec une petite réplique aujourd'hui- mais elle n'a jamais pris la même ampleur que ce qui s'est passé en France ou aux Pays-Bas, par exemple. Peut-être est-ce dû au fait que nous sommes un pays relativement petit, divisé par une barrière linguistique. Pour les fraudeurs, la Belgique ne constitue pas le 'marché' le plus attirant* »[356]. D'après J. De Blauwe, la Belgique peut aller plus loin en matière de détection des cyberincidents. En effet, « *Tout dysfonctionnement en cours ou passé reste très difficile à détecter avec précision. La solution pourrait [dès lors] venir de méthodes de détection plus performantes, de meilleurs algorithmes ou de techniques de mégadonnées* »[357]. Enfin, selon W. Coenraets, la Belgique peut encore mieux faire en matière de sensibilisation aux risques liés au numérique[358].

---

[348] S.n., « La Cybersécurité : nous sommes tous concernés », [2017] (https://www.febelfin.be/fr/newsletter360/9/table-ronde-complete, consulté le 15 janvier 2019).

[349] *Ibid.*

[350] Sénat de Belgique, *Demande d'établissement d'un rapport d'information relative à la nécessaire collaboration entre l'État fédéral et les entités fédérees en ce qui concerne les retombées, les opportunités, les potentialités et les risques de la 'société intelligente' numérique*, 24 mai 2018, p. 2 (session de 2017-2018 n°6-413/1)

[351] *Ibid.*, p. 4.

[352] *Ibid.*, p. 1.

[353] ITU, *Global Cybersecurity Index (GCI) 2017*, pp. 56-57, 60.

[354] *Ibid.*, p. 37.

[355] S.n., « La Cybersécurité : nous sommes tous concernés », [2017], *op. cit.*

[356] *Ibid.*

[357] *Ibid.*

[358] S.n., « La Cybersécurité : nous sommes tous concernés », *op. cit.*

Posture stratégique et bases légales

Cyberstratégie nationale

Depuis 2012, la Belgique dispose d'une stratégie fédérale de sécurité des réseaux et des systèmes d'information afin de garantir la cybersécurité de notre pays. Ce document propose de développer une cyberstratégie en trois piliers, d'ailleurs repris en 2014 dans l'accord gouvernemental de la Belgique[359]. Concrètement, il s'agit de mettre en place « *un cyberespace sûr et fiable qui respecte les valeurs et droits fondamentaux d'une société moderne ; veiller à une protection optimale contre la cybermenace des systèmes publics et infrastructures critiques [et enfin de] développer nos propres capacités de cybersécurité pour une politique de sécurité autonome et une réaction aux incidents sécuritaires adaptée* »[360]. Pour réaliser ces objectifs, la Belgique élabore une série de lignes d'action concrètes, comme le renforcement de la capacité à réagir aux cyberincidents, le développement des formations et campagnes de sensibilisation liées à la cybersécurité, l'amélioration de la protection contre la perturbation ou la violation des systèmes informatiques, la création d'un cadre légal pour répondre aux cyberattaques, ou encore la mise en place d'une approche centralisée et intégrée de la cybersécurité propice à la coopération nationale et internationale[361]. La révision de la cyberstratégie de 2012, initialement prévue pour l'été 2018[362], devrait avoir lieu au cours de l'année 2019.

La protection contre la cybermenace des infrastructures critiques (transport, énergie, télécommunications et finances) fait partie des objectifs stratégiques prioritaires de la Belgique[363]. La loi du 1er juillet 2011 impose en effet « *aux exploitants d'une infrastructure désignée comme critique de nommer un point de contact pour la sécurité mais également d'élaborer un P.S.E. (plan de sécurité de l'exploitant) visant à prévenir, atténuer, et neutraliser les riques d'interruption du fonctionnement ou de destruction de son infrastructure par la mise au point de mesures matérielles et organisationnelles internes* »[364]. Cette loi prévoit également que l'OCAM prenne en compte la cybersécurité dans l'analyse de la menace qu'il réalise, à la demande de la direction générale du Centre de crise[365]. En avril 2016, un rapport sur l'index de sécurité nucléaire pointe pourtant du doigt des manquements dans le domaine de la cybersécurité nucléaire en Belgique, laquelle obtient un score de 0 sur 4[366]. Suite à ces mauvais résultats, le CCB et l'Agence fédérale de contrôle nucléaire (AFCN) évaluent les actions à prendre afin de résoudre le problème[367]. Dès juillet 2014, la Commission européenne avait d'ailleurs exigé que les États membres transposent la « *directive sur la sûreté nucléaire européenne* » à leur propre législation, et ce pour le 15 août 2017 au plus tard[368]. En juin

---

[359] *Accord de gouvernement de la Belgique*, 9 octobre 2014, p. 148.

[360] *Cyber Security Strategy [of] Belgium*, 23 novembre 2012, p. 1.

[361] *Ibid.*, pp. 8-11.

[362] Interview de M. De Bruycker par E. Hoorickx le 28 mars 2018.

[363] *Cyber Security Strategy [of] Belgium*, 23 novembre 2012, pp. 6, 14.

[364] *Ibid.*, p. 14.

[365] *Ibid.*

[366] *Rapport sur les échanges de vues avec M. Miguel De Bruycker, directeur du Centre pour la Cybersécurité en Belgique*, 6 avril 2016, Chambre des représentants, DOC 54 1744/001, p. 23 ; *Rapport d'audition sur la cybersécurité des centrales nucléaires en Belgique*, Chambre des représentants de Belgique, 20 janvier 2017, DOC 54 2274/001, p. 6.

[367] *Ibid.*, p. 8.

[368] Directive 2014/87/ Euratom du conseil du 8 juillet 2014 modifiant la directive 2009/71/Euratom établissant un cadre communautaire pour la sûreté nucléaire des installations nucléaires, chapitre 2 bis, article 2.

2018, il ressort néanmoins d'une analyse réalisée par la Commission que « *la Belgique n'a notifié aucune mesure de transposition correspondant aux exigences spécifiques énoncées dans la directive. La Belgique dispose de deux mois pour répondre à l'avis motivé ainsi que pour adopter et communiquer toutes les mesures nécessaires pour garantir une transposition intégrale et correcte de la directive, faute de quoi la Commission pourrait saisir la Cour de justice de l'Union européenne* »[369]. La Belgique a depuis lors transposé cette directive, qui devrait être implémentée [pour 2019], après la publication d'un arrêté royal[370].

Dans le « Pacte national pour les Investissements Stratégiques » publié en septembre 2018, un comité stratégique recommande au gouvernement Michel d'investir 15 milliards d'euros dans la cybersécurité d'ici à 2030[371]. Parmi les initiatives concrètes suggérées, il y a la mise en place du portail d'échange « ISAC » qui permettrait aux entreprises de partager leurs meilleures pratiques en matière de cybersécurité[372] mais également l'amélioration de la prévention et de la résilience des services de sécurité, de police et de Défense face aux cyberincidents[373]. L'impact de l'évolution des technologies de l'information et de la communication (TIC) ne se limite en effet pas au domaine civil mais a également des répercussions significatives dans la sphère militaire.

Objectifs stratégiques de la Défense

La Défense dépend de plus en plus des nouvelles technologies numériques. Aucune armée moderne ne peut en effet fonctionner sans disposer de systèmes d'armes en réseau ou sans considérer le cyberespace comme un nouveau domaine opérationnel. Le développement récent de l'internet des objets a également un impact sur la cyberdéfense. Ainsi par exemple, les militaires belges en opération dans les Pays baltes ne devraient bientôt plus pouvoir utiliser leurs smartphones personnels par crainte d'espionnage par la Russie. En effet, l'application mobile Strava, très populaire pour enregister des activités sportives via GPS, livre encore trop souvent des informations sensibles sur les militaires et leur positionnement[374]. Désormais, les technologies numériques ne représentent plus seulement un outil de communication mais ouvrent également de nouvelles possibilités en termes offensif et défensif. Sur le terrain de la cyberguerre, les TIC sont devenues non seulement des outils de collecte du renseignement mais également des armes capables de réelles destructions physiques[375].

---

[369] http://europa.eu/rapid/press-release_MEMO-18-3986_fr.htm?locale=FR, consulté le 20 septembre 2018.

[370] Conférence au Collège de Défense à Bruxelles du Colonel Filip Gillet, chef de la direction Cyber d'ACOS IS, le 30 octobre 2018.

[371] F. Audag-Dechamps (sous la dir.), *Pacte national pour les Investissements Stratégiques*, septembre 2018, Bruxelles, pp. 3, 6 (https://premier.fgov.be/sites/default/files/articles/PNIS_Brochure_FR-WEB.pdf, consulté le 27 décembre 2018).

[372] FEB, *Agenda numérique 2.0*, juillet 2018 (https://www.feb.be/globalassets/publicaties/digitale-agenda-2.0/digitale-agenda-2.0-final-fr.pdf, p. 23, consulté le 27 décembre 2018).

[373] F. Audag-Dechamps (sous la dir.), *op. cit.*, p. 6.

[374] Belga, « Le smartphone restreint en opération militaire par crainte d'espionnage russe», 29 décembre 2018 (http://www.skynet.be/actu-sports/belgique/article/1914356/le-smartphone-restreint-en-operation-militaire-par-crainte-d-espionnage-russe, consulté le 29 décembre 2018)

[375] M. Fontaine et M. Benatar, « Cyber-attaques : aperçu du cadre juridique national », *Questions juridiques d'actualité en lien avec la défense*, 2017, p. 312.

Il est dès lors logique que l'aspect cybernétique fasse désormais partie d'une des quatre «dimensions capacitaires»[376] spécifiées dans la vision stratégique pour la Défense belge[377]. Selon ce document, celle-ci doit être en mesure d'apporter une réponse adéquate aux menaces cyber en développant une « *capacité cybernétique propre, composée d'un pilier défensif, offensif et du renseignement* »[378]. Ces objectifs stratégiques constituent le fil rouge de la stratégie de cybersécurité de la Défense, publiée en 2014 et qui devrait être revue au cours de l'année 2019[379]. Si le but ultime de la Défense en matière de cyberdéfense était, en 2014, de « *maintenir les risques dans le domaine cybernétique sous un niveau acceptable afin de garantir la bonne exécution de nos missions militaires* »[380], l'objectif actuel est double : améliorer la protection face aux menaces cyber mais également prendre conscience des opportunités qu'offre la cybersécurité. Celles-ci sont nombreuses, comme l'appui aux opérations conventionnelles ou à la diplomatie. Les actions cybernétiques permettent en effet de présenter des réponses proportionnelles aux attaques éventuelles. Enfin, l'arme cybernétique est multi-fonctionnelle. Elle peut être utilisée pour des opérations défensives et offensives mais également pour des actions de sabotage ou d'espionnage. Les actions cybernétiques peuvent dès lors engendrer des effets cinétiques et non cinétiques, avec un résultat immédiat et sans avertissement préalable.

En 2014, la Défense belge poursuivait quatre objectifs stratégiques : garantir un cyberespace sûr et protégé pour ses membres, appuyer toutes les missions et opérations de la Défense mais également celles des entités fédérées en fonction des moyens disponibles et enfin, améliorer la cybersécurité par une bonne coopération avec les acteurs internationaux tels que l'OTAN et l'UE[381]. La nouvelle cyberstratégie veillera également à renforcer la résilience de la Défense face aux cyberincidents en développant une véritable « culture d'hygiène cybernétique » auprès de son personnel et envisagera l'intégration du cyberespace comme nouveau domaine opérationnel. Sur ce dernier point, il s'agira de déterminer, conformément à la « taxonomie des opérations au sein du cyberespace » proposée par l'OTAN, les responsabilités de chacun en matière de cyberopérations défensives et offensives mais également en ce qui concerne les opérations liées à la cybersécurité et à celles relatives aux missions de renseignement, surveillance et reconnaissance (ISR-*Intelligence, Surveillance and Reconnaissance*) dans le cyberespace[382].

Un cadre légal en construction

Pour faire face aux cybermenaces, les autorités belges ont annoncé dès 2012 leur volonté de mettre en place, à partir de la législation existante, un cadre légal en matière de cybersécurité afin de trouver « *un équilibre entre les droits et les libertés des citoyens et les interventions indispensables de*

---

[376] Les quatre dimensions capacitaires de la Défense belge sont les composantes « Air », « Terre » et « Maritime », mais également le « Renseignement-Cyber Influence » (*La Vision stratégique pour la défense*, 29 juin 2016, pp.6-7).

[377] *Ibid.*, p. 99.

[378] *Ibid.*, p. 100.

[379] *Stratégie de cybersécurité pour la Défense*, 2014, p. 4 (ACST-Strategy-CyberSecurity-001, Ed 001/Rev 000/30-09-2014).

[380] *Ibid.*, p. 9.

[381] *Ibid.*

[382]

l'autorité »[383]. Depuis le 25 mai 2018, la nouvelle règlementation sur la protection des données à caractère personnel (RGPD) de l'Union européenne est applicable en Belgique[384]. Ce texte a donné lieu à la publication, en septembre 2018, de la « loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel »[385]. Le RGPD de l'UE prévoit en effet que les États membres puissent « *intégrer des éléments du présent règlement dans leur droit dans la mesure nécessaire pour garantir la cohérence et pour rendre les dispositions nationales compréhensibles pour les personnes auxquelles elles s'appliquent* »[386]. Ainsi par exemple, le RGPD dit que les États membres doivent définir une limite entre 13 et 16 ans, en dessous de laquelle un mineur devra avoir le consentement parental pour s'inscrire sur un réseau social. Les autorités belges ont fixé cette limite à 16 ans[387].

La Belgique fait également partie des pays qui se sont engagés, lors du Sommet de Varsovie, à considérer le cyberespace comme nouveau domaine opérationnel. La question de l'applicabilité du droit international au cyberespace fait d'ailleurs l'objet depuis 2013 d'un large consensus parmi les États. La prolifération des actions offensives dans l'espace numérique et les risques d'escalade des conflits liés aux erreurs d'attribution ou d'interprétation font du droit international un outil particulièrement essentiel à la préservation de la paix et de la sécurité internationales[388]. Selon le rapport du Groupe d'experts gouvernementaux des Nations unies (UNGGE) de 2013 et repris dans celui de 2015, « *le droit international et, en particulier, la Charte des Nations Unies sont applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique ouvert, sûr, pacifique et accessible* »[389].

La Belgique s'accorde sur la nécessité d'appliquer au cyberespace la législation internationale existante. La mise en place d'un cadre juridique national pour répondre aux cyberattaques devrait voir le jour prochainement. La seule mention de « cyberattaques » dans la loi du 30 novembre 1998[390], qui attribue, depuis le 4 février 2010, certaines compétences informatiques au département d'état-major

---

[383] *Cyber Security Strategy [of] Belgium*, 23 novembre 2012, p. 1.

[384] https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html?locale=fr, consulté le 15 janvier 2019.

[385] Le texte est disponible sur http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2018073046, consulté le 15 janvier 2019.

[386] « Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE », p. 2 § 8 (règlement général sur la protection des données) (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679, consulté le 15 janvier 2019).

[387] https://parismatch.be/actualites/societe/144495/protection-des-donnees-ce-quil-faut-savoir-nouveau-reglement-europeen, consulté le 15 janvier 2019.

[388] F. Douzet et S. Taillat, « Les enjeux de politique internationale. L'affirmation du leadership américain », dans S. Taillat, A. Cattaruzza et D. Danet, *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2018, p. 118.

[389] Document ONU A/68/98, § 19 (2013) (https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf, consulté le 28 décembre 2018); Document ONU A/70/174, §24 (2015) (https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf, consulté le 28 décembre 2018).

[390] Le contenu de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la modification intervenue par la loi du 4 février 2010 sont disponibles sur http://www.ejustice.just.fgov.be/eli/loi/1998/11/30/1998007272/justel , consulté le 16 janvier 2019.

Renseignement et Sécurité (ACOS IS)[391] ne suffit effectivement pas à pallier les lacunes dans le domaine[392]. Le concept de cyberattaque ne reçoit d'ailleurs aucune définition unanime en droit international. Alors que pour certains, ce concept implique nécessairement une destruction physique, pour d'autres, il implique uniquement la violation d'un système informatique[393]. Par ailleurs, l'article 167 de la Constitution stipule que c'est le Roi qui commande les forces armées et qui décide de l'engagement de celles-ci, afin de défendre l'intégrité territoriale du Royaume. Toute la difficulté consiste à déterminer dans quelle mesure une cyberattaque menace l'intégrité du territoire du Royaume[394]. Réagir de manière adéquate à une cyberattaque, dont l'attribution est loin d'être aisée à déterminer, nécessite un certain temps et l'approbation du Conseil des ministres, sur proposition du ministre de la Défense.

L'adoption par la Belgique de la directive de sécurité des réseaux et de l'information (SRI) de l'UE, mieux connue sous le nom de « directive NIS » (*Network and Information Security*) contribuera à la mise à jour nécessaire de la législation belge en matière de cybersécurité. En effet, la directive européenne exige que les États membres sanctionnent toute infraction aux dispositions nationales de cybersécurité et prennent toutes les mesures nécessaires pour que ces règles soient appliquées[395]. Le document impose notamment que « *Les États membres veillent à ce que les opérateurs de services essentiels notifient à l'autorité compétente ou au CSIRT [Computer Security Incident Respone Team], sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent* »[396]. Selon cette même directive, il est également prévu que « *Sur la base des informations fournies dans la notification de l'opérateur de servives essentiels, l'autorité compétente ou le CSIRT signale aux autres États membres touchés si l'incident a un impact significatif sur la continuité des services essentiels dans ces États membres. Ce faisant, l'autorité compétente ou le CSIRT doit, dans le respect du droit de l'Union ou de la législation nationale conformément au droit de l'Union, préserver la sécurité et les intérêts commerciaux de l'opérateur de services essentiels ainsi que la confidentialité des informations communiquées dans sa notification* »[397].

---

[391] L'acronyme SGRS est également utilisé pour désigner le service de renseignement et de sécurité des forces armées.

[392] M. Fontaine et M. Benatar, *op. cit.*, p. 313. Outre les missions de collecte et d'analyse, ACOS IS s'est vu octroyer, en 2010, la compétence de neutraliser les cyberattaques, d'en identifier les auteurs, ainsi que « *de réagir immédiatement par une propre cyber-attaque, dans le respect des dispositions du droit des conflits armés* » (*Ibid.*). Le champ d'application matériel de la disposition ne vise que les actions menées sur des systèmes d'information et de communication militaires ou ceux gérés par le ministre de la Défense (*Ibid.*, p. 341). L'arrêté royal du 21 décembre 2001 qui détermine la structure générale du Ministère de la Défense, sera adapté début 2019, afin notamment de préciser les missions du département d'état-major Operations et Entraînement (ACOS O&T) en matière de cybersécurité (http://www.ejustice.just.fgov.be/eli/arrete/2001/12/21/2002007001/justel, consulté le 16 janvier 2019). Le « cyberplan d'urgence nationale » de la Belgique désigne quant à lui les autorités responsables chargées de neutraliser les cyberattaques qui ne concernent pas la Défense, comme par exemple celles qui viseraient des infrastructures critiques.

[393] *Ibid.*, p. 320.

[394] *Ibid.*, pp. 341-343.

[395] *Ibid.*, p. 24.

[396] « Directive (UE) 2016/1148 du parlement européen et du conseil du 6 juillet concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information », dans l'Union, dans le *Journal officiel de l'Union européenne*, 19 juillet 2016, p. 20.

[397] *Ibid.*

Si certains considèrent que le cadre juridique relatif aux cyberattaques ne bénéficie pas encore de l'attention espérée[398], le code pénal belge sanctionne plus lourdement la cybercriminalité depuis août 2017. Conformément à la directive européenne concernant les attaques contre les systèmes d'information d'août 2013 (2013/40/UE), la Belgique a en effet relevé le seuil minimal des peines maximales infligées aux cybercriminels, notamment en cas d'attaque contre les infrastructures critiques[399]. L'attribution des actes de cybercriminalité est néanmoins compliquée, voire « *insoluble* »[400]. Le problème reste pourtant préoccupant puisque déjà en 2016, deux tiers des entreprises belges étaient victimes de cybercriminalité[401].

Selon Miguel De Bruycker certaines entreprises et organisations « *n'ont que trop peu conscience des risques, ne disposent pas d'expertise en la matière, pensent que cela ne leur arrivera pas ou estiment encore que l'investissement n'en vaut pas la chandelle* » [402]. D'après une étude réalisée par le leader mondial de la gestion des risques Marsh, pas moins de huit entreprises sur dix en Belgique n'auraient aucun plan pour contrer une cyber-attaque. Pourtant, 17% des entreprises belges auraient subi une attaque informatique fructueuse en 2016[403]. M. De Bruycker encourage dès lors toutes les organisations belges à adopter un plan de cybersécurité[404].

Actuellement, les entreprises belges sont principalement visées par des *ransomwares* et moins par le *phishing*, davantage utilisé au début des années 2010. W. Coenraets regrette néanmoins que les entreprises ne coopèrent pas davantage en matière de dénonciation de la cybercriminalité dont elles sont victimes. D'après M. De Bruycker, « *Nombre d'entreprises craignent en effet les fuites, mais nombreuses sont également celles qui doutent que leur déclaration contribue à identifier les auteurs ou leur vale une aide* » [405]. Il désire dès lors soutenir toute initiative qui favorise la volonté des entreprises de dénoncer les actes de cybercriminalité, même si la question de l'identification des auteurs reste très difficile. Selon Jan De Blauwe, le secteur financier belge souhaite que le signalement des incidents de cybercriminalité soit davantage centralisé afin de mieux cerner l'ampleur du problème et de se forger une expertise dans le domaine[406].

Le secteur bancaire semble davantage enclin à coopérer en matière de cybersécurité. La plupart des banques considèrent en effet que la mise en lumière de ces affaires de fraude permet de

---

[398] Ibid., p. 341.

[399] S.n., « Des peines plus sévères pour la cybercriminalité (art. 211-215 Pot-pourri V) », dans *Justement*, 18 octobre 2017, p. 6 (https://legalworld.wolterskluwer.be/media/5331/02-kl-justement-octo-2017-bdef.pdf, consulté le 16 janvier 2019 ; . *http://www.ejustice.just.fgov.be/mopdf/2017/07/24_1.pdf#Page481*, consulté le 12 octobre 2018.

[400] M. Fontaine et M. Benatar, « Cyber-attaques : aperçu du cadre juridique national », *Questions juridiques d'actualité en lien avec la défense*, 2017, p. 341.

[401] https://www.ccb.belgium.be/fr/actualit%C3%A9/en-2018-ne-laissez-aucune-chance-aux-cybercriminels, consulté le 17 octobre 2018.

[402] *Ibid.*

[403] Agence Belga, « Huit entreprises belges sur dix n'ont aucun plan pour faire face à une cyberattaque », *Le Vif.be*, 11 octobre 2018 (https://trends.levif.be/economie/entreprises/huit-entreprises-belges-sur-dix-n-ont-aucun-plan-pour-faire-face-a-une-cyberattaque/article-normal-1038631.html, consulté le 16 janvier 2019).

[404] *Ibid.*

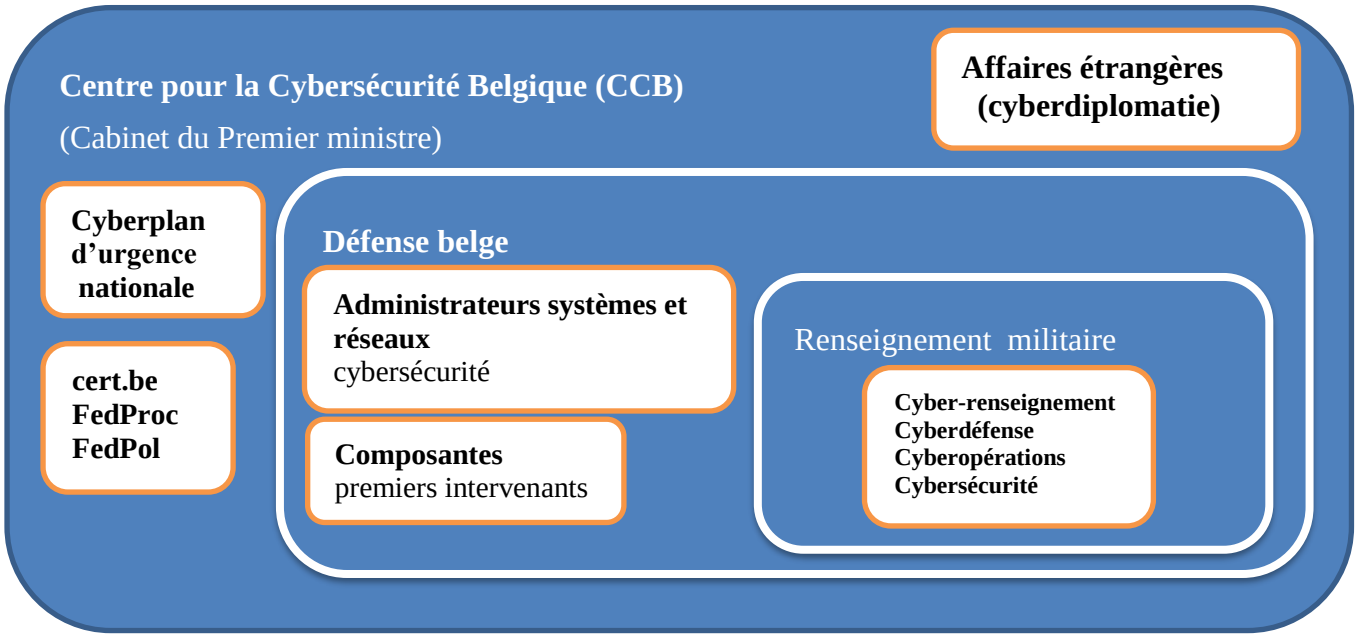
[405] *Ibid.*

[406] *Ibid.*

mieux cerner l'ampleur du problème et permet l'octroi de moyens nécessaires aux services publics concernés[407].

Dispositif capacitaire en matière de cybersécurité et cyberdéfense

Acteurs du cyberespace belge[408]



La Belgique dispose de différents organismes chargés de coordonner la politique sécuritaire du pays, quel que soit le degré de la menace[409]. En qualité d'autorité centrale, le « Centre pour la Cybersécurité Belgique » (CCB), créé par arrêté royal le 10 octobre 2014 et relevant de l'autorité du Premier ministre, est en charge de la cybersécurité en Belgique. Le CCB élabore la stratégie de cybersécurité pour la Belgique, assure la gestion de crise en cas de cyberincidents, en coopération avec le Centre de coordination et de crise du gouvernement, rend des avis sur la politique à suivre et prend des initiatives afin de conseiller et protéger les entreprises, les consommateurs et les pouvoirs publics[410]. L'objectif du CCB est de contribuer à un internet sûr et fiable et d'instaurer une politique nationale en collaboration avec les acteurs existants. Il s'agit par conséquent d'une mission de coordination entre les différents services publics[411]. Depuis 2018, le CCB compte 34

[407] *Ibid.*

[408] Tableau issu du briefing donné à l'École Royale Militaire de Bruxelles par le Colonel Filip Gillet, chef de la direction Cyber d'ACOS IS, le 30 octobre 2018.

[409] Il s'agit du Conseil National de Sécurité, responsable d'établir et de coordonner la politique générale du renseignement et de la sécurité du pays, du Centre Gouvernemental de Coordination et de Crise (CGCCR) qui garantit, 24 heures sur 24, la collecte et la diffusion aux instances compétentes de « *toutes les informations urgentes de toute nature* » et de l'Organe de Coordination pour l'Analyse de la Menace (OCAM) chargé d'effectuer des évaluations stratégiques et ponctuelles sur les menaces terroristes et extrémistes à l'encontre de la Belgique (www.premier.be; www.crisiscentrum.be).

[410] *Accord de gouvernement de la Belgique*, 9 octobre 2014, p. 148.

[411] *Rapport sur les échanges de vues avec M. Miguel De Bruycker, directeur du Centre pour la Cybersécurité en Belgique*, 6 avril 2016, Chambre des représentants, DOC 54 1744/001, p. 3.

membres, contre 10 en 2016[412]. M. De Bruycker estime que le CCB dispose de suffisamment de moyens et de budget pour réaliser les projets de cybersécurité en cours. Et d'ajouter que « *Les fonds sont disponibles et la volonté politique existe* », mais il faut du temps pour « *entreprendre les bonnes démarches* » [413].

Depuis 2017, le CCB gère l'« équipe d'intervention d'urgence en sécurité informatique » [414](ou « CERT-Computer Emergency Response Team » [415]) qui peut, en cas d'urgence informatique, coopérer avec « l'équipe d'intervention interinstitutionnelle de l'UE » (CERT-EU)[416]. C'est le parquet fédéral qui mène les enquêtes judiciaires, ouvertes par les *Computer Crime Units* régionales et fédérales de la police belge, relatives aux actes de piratages informatiques et cyberespionnage[417]. Depuis 2016, le ministère belge des Affaires étrangères dispose d'un cyberdiplomate, qui « *promeut une cyber économie digitale sûre* »[418]. En Belgique, 20% du PIB est actuellement développé par le marché digital[419].

Le CCB et le Centre de crise proposent, à travers un « cyberplan d'urgence nationale » rédigé en 2017, une réponse interdépartementale afin de protéger les intérêts vitaux du pays contre les cyberattaques. Ce plan décrit les missions des différents services dans la gestion des cybercrises et des cyberincidents [420]. Les 6 et 7 juin 2018, la « cellule cybersécurité du Centre de crise »[421] a d'ailleurs participé à un cyber-exercice international de grande ampleur, le *Cyber Europe 2018*-CE2018, organisé par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). A l'occasion de cet exercice, le Centre de crise a convié tous les acteurs nationaux concernés, à savoir le CCB, le CERT, ACOS IS, la « *Federal Computer Crime Unit* » (FCCU)[422],

---

[412] *Ibid.*, p. 11 ; *Rapport d'audition sur la cybersécurité des centrales nucléaires en Belgique*, Chambre des représentants de Belgique, 20 janvier 2017, DOC 54 2274/001, p. 7.

[413] S.n., « La Cybersécurité : nous sommes tous concernés », [2017] (https://www.febelfin.be/fr/newsletter360/9/table-ronde-complete, consulté le 15 janvier 2019).

[414]https://www.lachambre.be/kvvcr/showpage.cfm?section=qrva&language=fr&cfm=qrvaXml.cfm?legislat=54&dossierID=54-b096-860-0170-2016201712534.xml , consulté le 5 février 2019.

[415] Le « CERT » de la Belgique, mis en place en 2009, dépend du « *Centre pour la Cybersécurité Belgique* » depuis 2017 et a une double mission : d'une part, coordonner la gestion et la réponse aux incidents d'ampleur nationale auprès d'opérateurs d'infrastructures critiques ou de services essentiels ; et d'autre part, faire office de niche d'information en matière de cybersécurité (https://www.ccb.belgium.be/fr/actualit%C3%A9/transfert-cert-ccb , consulté le 5 février 2019).

[416] Le CERT-EU, opérationnelle depuis septembre 2012, veille à la cybersécurité des institutions européennes et collabore également avec différents CERT des États-membres (https://cert.europa.eu/cert/plainedition/en/cert_about.html).

[417] Briefing donné à l'École Royale Militaire de Bruxelles par le Colonel Filip Gillet, chef de la direction Cyber d'ACOS IS, le 30 octobre 2018.

[418] *Ibid.*

[419] *Ibid.*

[420] https://crisiscentrum.be/fr/content/cybersecurite-0, consulté le 12 septembre 2018.

[421] *Rapport d'audition du Lt-général Claude Van de Voorde, chef de SGRS, à la commission de la Défense nationale*, DOC 54 3267/001, 13 septembre 2018, p. 9 (http://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwi3yd3lkvLfAhUNzaQKHRC2DAAQFjAAegQICRAC&url=http%3A%2F%2Fwww.dekamer.be%2FFLWB%2FPDF%2F54%2F3267%2F54K3267001.pdf&usg=AOvVaw1srlEYXwZ7BJ53V37cmTrS, consulté le 16 janvier 2019).

[422] La *Federal Computer Crime Unit* (FCCU) est chargée de la lutte contre la criminalité ICT (Information and Communication Technology), « *entre autres pour protéger le citoyen des nouvelles formes de criminalité dans la société virtuelle. Cette mission consiste également à soutenir la lutte contre d'autres phénomènes criminels grâce à des enquêtes spécialisées dans des environnements ICT. La pédophilie sur l'Internet, les fraudes Internet (ventes*

l'IBPT (Institut belge des servicces postaux et des télécommunications), le SPF Mobilité et Transports, Belgocontrol et l'aéroport de Zaventem. L'exercice, dont les échos s'avèrent positifs fait l'objet d'une évalutation écrite[423]. En prévision des cybermenaces qui pesaient sur les élections communales d'octobre 2018 et celles qui menacent potentiellement les élections fédérales à venir, une *task force* de petite taille a été chargée de se concerter avec la cellule cybersécurité du Centre de crise afin de parer à de telles attaques[424]. Ce groupe de travail non permanent accorde une attention particulière aux cybermenaces russes et chinoises[425].

La Défense possède une des capacités cybernétiques les plus importantes du pays et contribue ainsi à la sécurité intérieure, en coordination avec le CCB[426]. Les administrateurs systèmes et réseaux assurent la sécurité et la sauvegarde des données du réseau informatique de la Défense. Les militaires des différentes composantes de la Défense doivent pouvoir détecter les cybermenaces et réagir de manière appropriée en cas de cyberincidents. Le reste de la capacité cybernétique de la Défense belge est centralisé au sein du département d'état-major Renseignement et Sécurité (ACOS IS). Celle-ci dispose d'une « direction cyber », elle-même subdivisée en six sections, chargées d'apporter une réponse adéquate en matière de cyber-renseignement, cyberdéfense, cyberopérations et cybersécurité[427]. Primo, la branche de « renseignement » s'occupe de l'évaluation de la menace cyber au sein des forces armées. Deuxio, le *Cyber Security Operations Centre* (CSOC) est chargé de la cyberdéfense des systèmes d'information et des communication (CIS) des forces armées belges[428]. Depuis 2016, cette capacité cybernétique bénéficie de moyens et personnel supplémentaires[429]. Tertio, et bien que la Belgique ne dispose pas encore de capacité cybernétique offensive, il existe une section « opérations » chargée de la développer, ce qui permettrait d'appuyer les opérations expéditionnaires depuis le territoire national (capacité de *reach back)*[430]. Il est prévu que la Défense soit capable de mettre sur pied des cyberactions offensives à partir de 2020-2025[431]. Quarto, la *National Distribution Agency* (NDA) est chargée de la cryptographie des messages émis au sein de la Défense et de la destruction du matériel classifié. Quinto, la section « accrédication » s'occupe, d'une part, de l'homologation des systèmes de communication et d'information (CIS) et d'autre part, de l'évaluation de la vulnérabilité des

---

frauduleuses sur l'Internet) et la fraude télécom relèvent également de ses compétences » (https://www.police.be/5998/fr/a-propos/directions-centrales/federal-computer-crime-unit, consulté le 16 octobre 2018).

[423]https://crisiscentrum.be/fr/news/planification-durgence/le-centre-de-crise-participe-un-cyber-exercice-international, consulté le 12 septembre 2018.

[424] *Rapport d'audition du Lt-général Claude Van de Voorde, chef de SGRS, à la commission de la Défense nationale*, DOC 54 3267/001, 13 septembre 2018, p. 9.

[425] *Ibid.*, p. 19.

[426] *La Vision stratégique pour la défense*, 29 juin 2016, p. 100. La Défense considère le CCB comme un « *organe de coordination national centralisé* » (*Stratégie de cybersécurité pour la Défense*, 2014, p. 11).

[427] Briefing donné à l'École Royale Militaire de Bruxelles par le Colonel Filip Gillet, chef de la direction Cyber d'ACOS IS, le 30 octobre 2018 ; J. Van Eyck, *De Belgische cyberdefensie en EU-samenwerking*, ERM, 2018, p. 34.

[428] J. Van Eyck, *op. cit.*

[429] *La Vision stratégique pour la défense*, 29 juin 2016, p. 100.

[430] *Ibid.*; J. Van Eyck, *op. cit.*, p. 34.

[431] *Rapport d'audition du Lt-général Claude Van de Voorde, chef de SGRS, à la commission de la Défense nationale*, DOC 54 3267/001, 13 septembre 2018, p. 19.

systèmes informatiques de la Défense. Sexto, la section « contrôle de la production » veille au suivi des tâches cybernétiques aux niveaux national et international[432].

La direction cyber de ACOS IS coopère également, au niveau national, avec le CERT, la Sûreté de l'État (service de renseignement civil belge), la « *Federal Computer Crime Unit* » (FCCU), le parquet fédéral et le « Centre de crise »[433]. Selon W. Coenraets, le recrutement de techniciens spécialisés en cybersécurité, singulièrement au sein de la police, constitue un défi majeur. La concurrence du privé en la matière, est, dit-il, énorme[434]. Selon une étude européenne réalisée en 2018, « *La Belgique souffre (…) d'une pénurie de professionnels qualifiés dans le domaine des TIC et ne se classe qu'à la 23e place européenne en ce qui concerne les diplômés des filières 'STEM' (sciences, technologie, ingéniérie et mathématiques)* »[435]. Néanmoins, afin d' « *enseigner aux jeunes adultes les compétences de base en codage et sécurité internet* », le gouvernement fédéral a consacré, en 2018, « *18 millions d'euros sur trois ans à des projets de formation aux compétences numériques* »[436]. En effet, « *La stimulation de l'adoption des technologies numériques combinée à une main-d'œuvre capable d'utiliser ces technologies pourrait permettre d'accroître davantage la productivité. Compte tenu de ce potentiel, le passage des entreprises et de l'industrie au numérique figure parmi les priorités des stratégies (…) au niveau fédéral comme dans les trois régions belges* »[437].

Coopération nationale et internationale

Travailler à la sécurité dans le cyberespace nécessite une très bonne coopération nationale mais également internationale. Cela suppose, de la part de toutes les parties, un échange mutuel d'informations et de bonnes pratiques en matière de cybersécurité mais également un engagement important, où des accords clairs s'imposent sur le rôle de tous les intéressés et la manière de collaborer ensemble[438]. La vitesse à laquelle le monde numérique se développe nécessite une coopération renforcée avec l'industrie et le monde académique, comme l'Institut Royal Supérieur de la Défense et l'École Royale Militaire[439]. Créé en janvier 2015, « la Cyber Security Coalition Belgium » réunit environ 40 entités des secteurs public et privé ainsi que du monde universitaire,

---

[432] J. Van Eyck, *op. cit.*, p. 34; *Rapport sur les échanges de vues avec M. Miguel De Bruycker, directeur du Centre pour la Cybersécurité en Belgique*, 6 avril 2016, Chambre des représentants, DOC 54 1744/001, p. 18.

[433] J. Van Eyck, *op. cit.*, p. 34. Créé en 1986, le Centre Gouvernemental de Coordination et de Crise (CGCCR) garantit une permanence ininterrompue, 24 heures sur 24 et 7 jours sur 7, pour la collecte, l'analyse et la diffusion aux instances compétentes de toutes « *les informations urgentes de toute nature* ». Il s'agit notamment des actualités relatives au terrorisme, aux cyber-incidents, à la santé publique, aux accidents ferroviaires, aux catastrophes naturelles ou au nucléaire (www.crisiscentrum.be).

[434] S.n., « La Cybersécurité : nous sommes tous concernés », [2017] (https://www.febelfin.be/fr/newsletter360/9/table-ronde-complete, consulté le 15 janvier 2019).

[435] S.n., « Indice relative à l'économie et à la société numériques (DESI-[*Digital Economy and Society Index*]) 2018-Rapport par pays: Belgique», s.d., p.6 (https://ec.europa.eu/digital-single-market/en/scoreboard/belgium, consulté le 3 février 2019).

[436] *Ibid.* , p. 7.

[437] *Ibid.*, p. 9.

[438] *Cyber Security Strategy [of] Belgium*, 23 novembre 2012, p. 8.

[439] *Stratégie de cybersécurité pour la Défense*, 2014, pp. 13-14 (ACST-Strategy-CyberSecurity-001, Ed 001/Rev 000/30-09-2014).

et vise à renforcer la cybersécurité au niveau national par le biais de 4 axes stratégiques, à savoir le partage d'expérience, la collaboration opérationnelle, les recommandations politiques et les campagnes de sensibilisation[440]. Selon W. Coenraets, cette coalition devrait également cibler les entreprises qui collectent une grande quantité de données[441].

L'État belge possède en outre deux instruments de concertation en matière de sécurité de l'information. Il s'agit d'une part de la plateforme Belnis, qui se concentre sur la sécurité des réseaux informatiques pilotée par Fedict (le Service public fédéral Technologie de l'Information et de la Communication) et d'autre part, de l' « *Information Security Management Forum* » (ISMF) mis en place en 2011[442]. Ce forum contribue à « *harmoniser les visions des différentes institutions [fédérales] participantes et a déjà produit plusieurs guides et documents en matière de sécurité de l'information* »[443]. M. De Bruycker souhaiterait aller plus loin et permettre à la CERT belge de gérer « *une plateforme efficace pour l'échange d'informations entre tous les acteurs à propos des menaces, des vulnérabilités et des incidents* »[444].

La Belgique s'efforce également de respecter ses engagements euro-atlantiques relatifs à la cybersécurité et la cyberdéfense. De nombreuses mesures de protection ne sont en effet efficientes que si elles peuvent être projetées au niveau international[445]. La directive de sécurité des réseaux et de l'information (SRI) de l'UE, mieux connue sous le nom de « directive NIS » (*Network and Information Security*) et adoptée le 6 juillet 2016, fixe de nouvelles obligations en matière de cybersécurité aux États membres et à certaines entreprises afin de créer un cyber environnement fiable au sein de l'UE[446]. Les trois objectifs principaux de cette directive sont la mise en place par tous les États membres d'un minimum de moyens nationaux pour favoriser la cybersécurité par l'établissement d'autorités compétentes et l'adoption de stratégies et de plans de coopération; le développement, par ces mêmes autorités, d'un réseau permettant un échange coordonné d'informations ainsi que la détection des menaces cybernétiques et l'intervention en cas de menaces et incidents au sein de l'UE; et enfin, le partage d'informations entre le secteur privé et le secteur public afin d'adopter des mesures appropriées et proportionnées pour garantir la SRI et signaler aux autorités compétentes tout incident de nature à compromettre sérieusement leurs systèmes informatiques et à avoir un impact significatif sur la continuité des services critiques et la fourniture des biens[447]. Il est prévu que la directive s'applique aux opérateurs de « services essentiels »[448] et

---

[440] Rapport d'activité 2016 du Cyber security coalition, Bruxelles, pp. 3, 5.

[441] S.n., « La Cybersécurité : nous sommes tous concernés », *op. cit.*

[442] *Stratégie de cybersécurité pour la Défense*, 2014, p. 13 (ACST-Strategy-CyberSecurity-001, Ed 001/Rev 000/30-09-2014) ; *Question et réponse écrite n°0146-Législature 53*, Chambre des représentants de Belgique, juin-juillet 2013.

[443] *Ibid.*

[444] S.n., « La Cybersécurité : nous sommes tous concernés », *op. cit.*

[445] *Cyber Security Strategy [of] Belgium*, 23 novembre 2012, p. 8.

[446] « Directive (UE) 2016/1148 du parlement européen et du conseil du 6 juillet concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information », dans l'Union, dans le *Journal officiel de l'Union européenne*, 19 juillet 2016.

[447] Proposition de résolution visant à renforcer la cybersécurité en Belgique, Chambre des représentants de Belgique, 16 septembre 2014, DOC 54 0257/001, p. 5.

[448] Un opérateur de service essentiel est une « *entité [qui] fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques ; la fourniture de ce service est tributaire des réseaux et des systèmes d'informations ; et un incident aurait un effet disruptif important sur la fourniture dudit service* ». (Directive (UE) 2016/1148 du parlement européen et du conseil du 6 juillet concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dans *Journal*

aux fournisseurs de service numérique[449]. Les États membres sont dès lors chargés d'établir quelles sont les entités qui remplissent les critères de la définition d'un opérateur de services essentiels[450]. La directive exige également que « *Les États membres fixent des règles relatives aux sanctions applicables en cas d'infraction aux dispositions nationales adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour que ces règles soient appliquées* »[451]. Bien que l'adoption du document par les États membres ait été prévue pour le 9 mai 2018 au plus tard, la Belgique devrait atteindre cet objectif pour le début de l'année 2019[452]. Un projet de loi a été émis le 12 novembre 2018 afin de transposer la directive NIS[453]. Après son adoption par le Parlement, le texte sera soumis au Roi pour être sanctionné et promulgué. Il est également prévu que la Belgique revoie sa cyberstratégie à la lumière de la directive SRI[454]. La mission est chapeautée par le « *centre pour la cybersécurité Belgique* »[455]. Il s'agira notamment de définir le rôle et les responsabilités des différents acteurs concernés[456].

La Belgique fait également partie des 11 États membres (Belgique, Allemagne, Estonie, Irlande, Grèce, Lettonie, Pays-Bas, Autriche, Portugal, Finlande et Suède) qui participent au projet « Cyber Ranges Federation » (ou fédération des plateformes informatiques de simulation en matière de cybersécurité[457]), lancé dans le cadre du programme de mise en commun et de partage de

---

officiel de l'Union européenne, 19 juillet 2016, p. 14). Plus concrètement, les services essentiels sont les secteurs d'infrastructures critiques (énergie, transports, banques et infrastrucutures numériques) mais également les secteurs liés aux marchés financiers, à la santé et à la fourniture et distribution d'eau potable (*Ibid*., pp. 27-29 ; *Proposition de résolution visant à renforcer la cybersécurité en Belgique*, Chambre des représentants de Belgique, 16 septembre 2014, DOC 54 0257/001, p. 6 ; *Rapport d'audition sur la cybersécurité des centrales nucléaires en Belgique*, Chambre des représentants de Belgique, 20 janvier 2017, DOC 54 2274/001, p. 4).

[449] Directive (UE) 2016/1148 du parlement européen, *op. cit.*, p. 2.

[450] *Ibid.*, p. 4.

[451] *Ibid.*, p. 24.

[452] ECSA (*European Corporate Security Association*) Info session, 30 mai 2018.

[453] Chambre des représentants de Belgique, *Projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt general pour la sécurité publique*, Bruxelles, 12 novembre 2018 (DOC 54 3340/001) (http://www.dekamer.be/FLWB/PDF/54/3340/54K3340001.pdf, consulté le 29 décembre 2018).

[454] *Ibid.*

[455] A. Dammekens, *Cybersécurité- la directive européenne impose aux entreprises l'obligation de notifier les cyberincidents*, 12 juillet 2016 (consultable sur www.vbo-feb.be). Le « *Centre pour la Cybersécurité Belgique* », créé en octobre 2014 et relevant de l'autorité du Premier ministre, est chargé d'élaborer une stratégie de cybersécurité pour la Belgique, d'assurer la gestion de crise en cas de cyberincidents, en coopération avec le Centre de coordination et de crise du gouvernement, de rendre des avis sur la politique à suivre et de prendre des initiatives afin de conseiller et de protéger les entreprises, les consommateurs et les pouvoirs publics (*Accord de gouvernement de la Belgique*, 9 octobre 2014, p. 148 ; www.ccb.belgium.be).

[456] Interview de M. De Bruycker par E. Hoorickx le 28 mars 2018 ; *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, p. 16.

[457] *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense* , 2018, § 8 (2018/2004 (INI)-P8-TA-PROV (2018)0258); https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states, consulté le 29 décembre 2018.

l'Agence européenne de Défense (AED)[458]. Cette fédération vise à améliorer la qualité de la formation et des exercices de cyberdéfense au sein de l'UE[459].

La Belgique participe également, comme pays observateur, à deux projets cyber de la Coopération structurée permanente (CSP). Ceux-ci ont fait l'objet d'un accord politique au Conseil des Affaires étrangères de l'Union européenne en décembre 2017. La Belgique peut ainsi suivre l'évolution des deux programmes et les rejoindre plus ou moins rapidement le cas échéant. Le premier projet concerne la mise en place d'une plateforme de partage d'informations sur la réponse à apporter aux attaques et menaces cyber (*Cyber Threats and Incident Response Information Sharing Platform*). Le second projet concerne la création d'équipes de réaction rapide aux attaques cyber et l'assistance mutuelle dans la cybersécurité (*Assistance in Cybersecurity and Cyber Rapid Response Teams*-CRRT). Ces équipes d'intervention rapide permettent aux États membres de s'entraider afin de garantir un niveau plus élevé de cyber-résilience et de répondre collectivement aux incidents cybernétiques[460].

La problématique de la « *cyberdéfense* » est également au cœur des préoccupations de l'OTAN. L'Alliance atlantique dispose d'ailleurs, depuis 2008, d'un centre d'excellence pour la cyberdéfense situé à Tallinn, en Estonie. Celui-ci mène des exercices mais également des activités de recherche et de formation dans des domaines techniques, juridiques et stratégiques liés à la cybersécurité[461]. Depuis janvier 2017, la Belgique participe aux activités du centre d'excellence pour la cyberdéfense situé à Tallinn, en Estonie, aux côtés de seize autres pays de l'Alliance atlantique[462].

C'est également à l'initiative de la Belgique que le projet de plateforme d'échange d'informations sur les logiciels malveillants (MISP- *Malware Information Sharing Platform*) a été lancé à l'OTAN, en novembre 2013. Le but ultime du projet est de développer une capacité OTAN accessible à tous les pays membres, par l'intermédiaire de laquelle ils s'engagent à partager leurs informations sur les caractéristiques techniques des logiciels malveillants, sans pour autant que des précisions soient données sur l'attaque proprement dite[463]. En avril 2017, la Belgique a également avalisé le *Memorandum of Understanding* (MoU) relatif à la coopération en matière de cyberdéfense entre les pays Alliés et l'OTAN afin d'améliorer la prévention et la résilience en cas de cyberincidents[464].

Outre ces collaborations internationales, la Belgique coopère principalement avec le Benelux et la France pour la cybersécurité. Notre pays a ainsi obtenu du Luxembourg un outil

---

[458] *Ibid.*, § 27.

[459] https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/09/13/cyber-ranges-federation-project-reaches-new-milestone, consulté le 29 décembre 2018.

[460] https://club.bruxelles2.eu/2017/12/la-pesco-comportera-18-projets-la-liste-definitive/, consulté le 17 octobre 2018.

[461] https://ccdcoe.org/about-us.html.

[462] S.n., *La Belgique a rejoint le centre d'excellence de l'Otan pour la défense cybernétique,* www. rtbf.be, 26 avril 2016.

[463] https://www.nato.int/cps/fr/natohq/news_105485.htm?selectedLocale=fr, consulté le 10 octobre 2018.

[464] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf; https://www.presscenter.org/fr/pressrelease/20170428/memorandum-of-understanding-entre-lotan-et-la-belgique-concernant-la-cooperati, consulté le 16 janvier 2019.

d'analyse de risque, baptisé Monarch. Des dipositions sont également prises avec les Pays-Bas afin d'améliorer les échanges d'informations relatives aux cybermenaces[465].

Hygiène informatique nationale

Afin d'améliorer la cyberhygiène[466] de son pays, le gouvernement belge promeut également les formations et campagnes d'information afin d'améliorer « *l'expertise et les connaissances des différents acteurs du cyberespace relatives à la cybersécurité* »[467]. Ainsi, un premier master en cybersécurité a été lancé en Fédération Wallonie-Bruxelles à la rentrée 2016-2017. Cette formation, dispensée conjointement à Namur et à l'ULB, a pu être mise en place grâce à la collaboration entre six établissements d'enseignement supérieur, universités et hautes écoles.[468]. Les universités et hautes écoles de Flandre ne proposent pas encore ce type de master mais bien un certain nombre de cours en la matière[469]. En outre, depuis quelques années, un *cybersecurity challenge* est organisé en Belgique afin de permettre aux étudiants belges en informatique de s'affronter et se faire connaître dans le domaine professionnel de la cybernétique[470].

Des projets sont également en cours pour améliorer la formation cyber des différents acteurs de la Défense. Il est notamment prévu que les cours existant au sein des écoles militaires intègrent des aspects cyber. Une politique de personnel et de formation adaptée est également mise sur pied en vue d'aquérir suffisamment d'expertise en cybersécurité et de la conserver. Pour ce faire, le recours aux réservistes et stagiaires du secteur TIC (Technologies de l'information et de la communication) civil est envisagé[471]. Le personnel civil et militaire de la Défense sont annuellement évalués en termes de cybersécurité, dans le cadre du *Joint Individual Common Core Skills Training.* Enfin, les capactiés de recherche et de développement sont développées par le biais des structures existantes au sein de la Défense, comme l'Institut Royal Supérieur de Défense (IRSD)[472].

Ces formations sont renforcées par des campagnes de sensibilisation. En 2016, le CCB a ainsi permis l'ouverture du site *safeonweb.be,* dont l'ambition est d' « *informer rapidement et*

---

[465] S.n., « La Cybersécurité : nous sommes tous concernés », [2017] (https://www.febelfin.be/fr/newsletter360/9/table-ronde-complete, consulté le 15 janvier 2019).

[466] Terme utilisé dans la *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense* , 2018, § 32 (2018/2004 (INI)-P8-TA-PROV (2018)0258)

[467] *Cyber Security Strategy [of] Belgium*, 23 novembre 2012, p. 2.

[468] Il s'agit de l'Université libre de Bruxelles (ULB), l'Université catholique de Louvain (UCL), l'université de Namur (UNamur), l'École royale militaire (ERM), l'Institut des hautes études de Belgique et la Haute école libre de Bruxelles Ilya Prigogine (HELB) (J. Thomas, « Gros succès pour le master en cybersécurité », 11 octobre 2017, dans *Dhnet.be*, consulté le 22 ocotbre 2018) ; D. Brichard, « La cybersécurité, le secteur où l'on s'engage », 24 mars 2018, dans *rtbf.be*, consulté le 22 octobre 2018.

[469] Pour plus de détails relatifs aux formations en sécurité informatique proposées en Belgique, voir : https://www.ccb.belgium.be/fr/ict-security-education-belgium.

[470] D. Brichard, « La cybersécurité, le secteur où l'on s'engage », 24 mars 2018, dans *rtbf.be,* consulté le 22 octobre 2018.

[471] *Stratégie de cybersécurité pour la Défense*, 2014, pp. 11-12 (ACST-Strategy-CyberSecurity-001, Ed 001/Rev 000/30-09-2014).

[472] *Ibid.*, p. 14.

efficacement les citoyens belges en matière de sécurité informatique, des plus récentes et plus importantes menaces numériques et de sécurité sur Internet »[473].

[473] https://safeonweb.be/fr/home, consulté le 22 octobre 2018.

Conclusions et recommandations

Les constats

Des risques cybernétiques toujours plus complexes et préoccupants

Depuis quelques années, les cyberattaques font partie des risques dont la probabilité de survenance est la plus élevée à travers le monde, au même titre que les catastrophes naturelles, les mouvements de migration à grande échelle, les conflits interétatiques ou les attaques terroristes. Les entreprises européennes sont quotidiennement victimes de cyberattaques et les réseaux de l'OTAN, ainsi que ceux liés à l'Organisation mais non protégés par elle, font également l'objet d'un ciblage croissant. La complexification des piratages informatiques, comme le développement du cyber combat autonome, sont des réalités qu'il convient de prendre en compte. D'aucuns envisagent d'ailleurs, certes de façon sans doute exagérée, l'éventualité d'un « Cyber Pearl Harbor » ou un « 9/11 numérique ».

Il semble acquis, depuis une dizaine d'années, que les conflits militaires ne peuvent plus se concevoir sans atteinte aux systèmes d'information. Les cyberattaques qui frappent l'Estonie en 2007, et la Géorgie en 2008 utilisent significativement les technologies de l'information et des communications pour parvenir à l'hégémonie politique et militaire, notamment par le recours à des moyens offensifs. Plus inquiétant encore, les cyberattaques peuvent désormais avoir des effets aussi neutralisants que ceux des armes conventionnelles, comme l'a démontré la cyberagression contre le programme nucléaire iranien en 2010. La problématique de la cyberdéfense représente donc un nouveau défi dans le concept stratégique de l'OTAN. L'UE publie, quant à elle, sa première stratégie de cybersécurité en 2013.

Depuis la crise russo-ukrainienne de 2014, caractérisée par le recours aux armes numériques dans un contexte de guerre hybride, l'OTAN considère qu'il revient au Conseil de l'Atlantique Nord de décider, au cas par cas, des circonstances d'une invocation de l'article 5, à la suite d'une cyberattaque. L'UE envisage quant à elle la possibilité d'appliquer, le cas échéant, la clause d'assistance mutuelle et celle dite de solidarité, prévues dans ses traités. Déterminer juridiquement si une cyberattaque peut être considérée comme une agression armée n'est cependant pas chose aisée et est loin de faire l'unanimité. La question de l'attribution est également compliquée à résoudre.

Une stratégie euro-atlantique difficile à mettre en oeuvre

Dans un contexte de gestion de crise, la nécessité de sécuriser les mécanismes d'information et de communication de l'OTAN et de l'UE apparaît de plus en plus clairement. Les deux organisations ont ainsi récemment reconnu le cyberespace comme nouveau domaine d'opérations, à l'instar des espaces terrestre, aérien et maritime. Pour prévenir et faire face aux cyberattaques, l'UE et l'OTAN ont également décidé, dès 2016, de mettre en commun un certain nombre d'informations liées à la cyberdéfense. Cette coopération permet notamment d'éviter la redondance des activités et capacités des deux institutions. La cyberstratégie euro-atlantique se heurte néanmoins à un enjeu crucial : le rôle déterminant des États dans la protection des systèmes d'information et dans la réponse stratégique à apporter en cas de cyberattaque de l'un d'eux. D'une part, une sécurisation des CIS nationaux non suffisamment zélée est susceptible de porter atteinte à l'exécution des tâches fondamentales de l'UE et de l'OTAN, un constat qui s'applique également aux compagnies privées, contrôlant actuellement une grande partie du cyberespace. L'auto-évalutation annuelle des États otaniens en matière de cyberdéfense et la transposition de la directive européenne SRI témoignent de cette prise de conscience. D'autre part, les États peuvent jouer un rôle important dans la manière de répondre à une

cyberattaque dont serait victime un pays allié qui, le cas échéant, invoquerait le difficilement applicable article 5. En définitive, force est de constater que la stratégie de cyberdéfense euro-atlantique se heurte encore à de nombreuses difficultés et reste compliquée à mettre en œuvre.

Les États, comme cyberpuissances vulnérables

Les États restent les premiers responsables de la protection de leurs systèmes d'information et dans la réponse stratégique à apporter en cas de cyberattaque. La cybersécurité est en effet essentielle pour assurer prospérité et sécurité à leurs citoyens. Évaluer la capacité d'un État à agir dans le cyberespace diffère selon les critères choisis et reste difficile. En effet, rares sont les études liées à l'évolution des cyberagressions visant les particuliers, les entreprises ou plus globalement les pays. Ce constat s'explique sans doute par la relative nouveauté du phénomène cybernétique. Par ailleurs, l'origine des cyberattaques ne peut pas toujours être établie avec certitude et n'entraîne pas nécessairement l'assentiment des autorités de l'État en question. Enfin, les pays et les entreprises rechignent souvent à dévoiler les cyberattaques dont elles sont victimes et ont tendance à sous-estimer le coût global de celles-ci.

Malgré la difficulté d'évaluer la capacité d'un État à assurer sa cybersécurité, il apparaît néanmoins que la cyberpuissance d'un pays se traduit par une capacité industrielle et un potentiel scientifique importants dans le domaine numérique, un degré de connectivité élevé, une forte centralité de ses réseaux informatiques sur la scène internationale et une capacité à utiliser les moyens financiers et techniques des grands acteurs privés, détenteurs d'un potentiel numérique important. Une cyberpuissance doit également être en mesure d'assurer efficacement sa propre cybersécurité et sa cyberdéfense. Pour ce faire, elle doit adopter une cyberstratégie qui s'articule autour d'une bonne compréhension des cybermenaces, un renforcement de la prévention et de la résilience à celles-ci, des moyens destinés à la recherche et la formation, une hygiène informatique nationale, une adéquation du cadre légal pour réagir aux cyberattaques, mais également une coopération internationale et nationale en matière de cyberdéfense et de cybersécurité, en ce compris un partenariat entre le secteur public et le secteur privé. Enfin, une cyberpuissance doit posséder un dispositif organisationnel capable d'assurer la mise en œuvre et le contrôle de la bonne application de sa posture stratégique en matière numérique.

Le facteur humain fait également partie des priorités de la cybersécurité. En effet, les cybercriminels visent généralement moins les systèmes que les utilisateurs. Souvent, les fraudeurs n'essayent pas de déjouer les serveurs extrêmement sécurisés mais visent plutôt les internautes, singulièrement dans les attaques au *ransomware*. D'aucuns considèrent d'ailleurs que la nouvelle règlementation sur la protection des données à caractère personnel de l'Union européenne encouragerait les criminels à s'en prendre à des internautes lambda plutôt qu'à des systèmes très protégés.

Certains estiment que plus les capacités cyber offensives et défensives des pays sont élevées et leur dépendance cybernétique faible, plus ces États dominent le cyberespace. En réalité, la cyberpuissance se mesure à l'aptitude et à la volonté, d'une part, d'employer pleinement ses capacités cybernétiques et, d'autre part, de décourager le recours aux cyberattaques en augmentant la difficulté, le coût et le risque pour un agresseur.

En outre, il existe une certaine corrélation entre le niveau de puissance classique (économique, technologique et militaire) et le niveau de cyberpuissance. Ainsi, les États-Unis constituent la nation otanienne la plus performante en matière de cybersécurité. Le leadership américain sur le cyberespace illustre néanmoins une double dynamique paradoxale. Elle se traduit en effet par la promotion de normes en faveur de la réduction des risques liés à la conflictualité numérique mais également par une militarisation du cyberespace qui engendre de l'instabilité. Le pays de l'Oncle Sam est, à l'échelle planétaire, l'État le plus agressif cybernétiquement mais également la deuxième nation victime du plus

grand nombre de cyberattaques. Il est intéressant de constater que la Chine, considérée comme le pays le plus belliqueux en matière cyber, ne fait pas partie des 10 pays les plus attaqués cybernétiquement et que la Russie arrive seulement en 7e position des États les plus touchés par les cyberattaques.

La France, le Royaume-Uni et l'Allemagne, considérés comme des cyberpuissances européennes à la pointe en matière de cybersécurité, s'avèrent également particulièrement vulnérables aux cyberattaques. La quantité des piratages numériques est en effet proportionnelement plus élevée dans les pays où le nombre de personnes connectées est le plus important. Il n'est donc pas surprenant que la république de Singapour, nation la plus connectée au monde et la plus performante en matière de cybersécurité, n'ait pu empêcher, en juillet 2018, qu'un quart de sa population soit victime de vols de données personnelles suite à la pire des cyberattaques de son histoire. De même, l'Estonie, pays également hyperconnecté, et considéré comme l'État européen le plus performant en matière de cybersécurité, a dû suspendre, en novembre 2017, les certificats de sécurité d'environ 60% des cartes d'identité électroniques nationales munies d'une puce défectueuse afin de réduire le risque de vols d'identité.

La Belgique, un pays relativement mature en matière de cybersécurité

Selon une étude de 2017, qui évalue le niveau de cybersécurité des 28 États membres de l'UE, la Belgique occupe la 10e position du classement. La coopération nationale et internationale mais également la capacité de résilience et de prévention constituent les points forts de notre pays. C'est en effet à l'initiative de la Belgique que le projet de plateforme d'échange d'informations sur les logiciels malveillants (MISP) a été lancé à l'OTAN, en novembre 2013. En outre, à l'échelle planétaire, notre pays enregistre un des taux d'adoption les plus élevés du protocole Internet IPv6, qui permet d'attribuer une adresse IP unique à chaque utilisateur, ce qui présente des avantages évidents en matière de répression et d'enquêtes sur la cybersécurité.

La Belgique est également un des pays dont le pourcentage d'internautes est le plus élevé et elle fait partie des États au degré de connectivité le plus important. Les réseaux informatiques civils et militaires de la Belgique sont en permanence confrontés à des incidents cybernétiques. L'État belge ne constitue néanmoins pas le marché le plus attirant pour les cyberattaques. La relative petitesse du pays et la barrière linguistique sont sans doute pour beaucoup dans cette réalité.

Le défi actuel des autorités belges consiste à ajuster les moyens juridiques, organisationnels et techniques existants afin de disposer d'une réponse appropriée face aux cybermenaces. Si les fonds sont disponibles et la volonté politique existe, il faut cependant du temps pour atteindre de tels objectifs. Ainsi, la révision de la cyberstratégie nationale initialement prévue pour l'été 2018, devrait voir le jour en 2019. La transposition de la directive nucléaire européenne à la législation belge, exigée pour l'été 2017 n'a été réalisée qu'à la fin de l'année 2018. Enfin, l'adoption par la Belgique de la directive SRI, prévue pour début mai 2018 au plus tard, devrait être effective début 2019.

À côté de ses engagements euro-atlantiques en matière de cybersécurité et de cyberdéfense, la Belgique coopère singulièrement avec le Benelux et la France dans le domaine numérique. Notre pays a ainsi obtenu du Luxembourg un outil d'analyse des risques cybernétiques, baptisé Monarch. Des dipositions sont également prises avec les Pays-Bas afin d'améliorer les échanges d'informations relatives aux cybermenaces.

Les recommandations

Mener une réflexion de fond sur le numérique

L'objectif actuel en matière de cybersécurité est double : améliorer la protection des menaces cyber mais également prendre davantage conscience des opportunités offertes par le numérique. Il

semble en effet opportun d'examiner les conséquences et les effets juridiques et éthiques de cette révolution technologique, sans pour autant étouffer l'innovation. Si la numérisation de notre société offre de nombreuses opportunités, elle comporte également des risques qui nécessitent attention et initiatives de la part des décideurs politiques. L'apparition de nouveaux emplois dans des secteurs qui jusqu'ici n'existaient pas, comme la lutte contre la cybercriminalité ou le *blockchain* mais également la stimulation d'un nouvel entreprenariat avec de nouveaux produits, font partie des avantages liés au développement du numérique. Parmi les défis à relever sur le plan de la cybersécurité, il y a notamment la nécesssité d'améliorer le cryptage des données ainsi que le problème du respect de la vie privée. La question des « big data » fait également partie des enjeux cruciaux. En effet, si les données massives, et les algorithmes qui y sont liés, facilitent certaines activités de renseignement, ils ne peuvent pas remplacer le rôle essentiel des humains dans les questions de sécurité nationale.

L'intelligence artificielle (IA) mise au service du numérique fait également partie des enjeux à prendre en compte. Certains considèrent en effet que l'IA peut permettre de remplacer l'expertise humaine, de détecter les incidents de cybersécurité de façon beaucoup plus certaine, de répondre automatiquement aux attaques et enfin de s'adapter rapidement à l'augmentation des volumes de données traitées. D'autres mettent néanmoins en garde contre le danger d'une démocratisation du développement technique qui aboutirait à renforcer l'emprise de certains acteurs sur celui-ci. L'autonomisation des machines détournerait en effet l'attention d'enjeux de pouvoir qui se posent dès à présent, à savoir que cette autonomisation intensifie également la concentration de la décision dans les mains de certains. En définitive, il s'agit de s'interroger sur la légitimité d'une réponse automatique aux cyberattaques, fondée sur l'IA plutôt que sur une évaluation humaine éthique et juridique.

Renforcer la résilience internationale dans le respect du droit international

Il paraît de plus en plus nécessaire de mettre en place un cadre normatif paneuropéen unifié pour la cybersécurité afin de faciliter les réactions face aux cyberincidents. Il serait également judicieux d'établir une norme de qualité européenne pour les fournisseurs de technologies.

L'OTAN et l'UE devraient davantage s'accorder sur l'assimilation juridique d'une cyberattaque à une agression armée afin d'éviter une réaction illégale. Le recours au Conseil de sécurité s'avère indispensable dans cette démarche. L'opérationnalisation du rapport UNGGE de 2015 pourrait également ouvrir la voie à une acceptation plus large de la notion d'agression armée et étendre les situations dans lesquelles le droit de légitime défense pourrait être invoqué. En définitive, il conviendrait que les États se mettent d'accord sur la manière dont il faudrait qualifier juridiquement les cyberattaques et sur les mesures que les pays doivent mettre en œuvre pour faire face à celles-ci. L'interprétation et la mise en œuvre de l'obligation de diligence des États constituent également un défi majeur dans l'application du droit international aux cyberopérations.

Les pays alliés de l'OTAN devraient approfondir la réflexion sur la mise en œuvre de l'article 5. Faut-il riposter par une cyberdéfense active et/ou par une réponse conventionnelle ? Ou doit-on au contraire privilégier la cyberdiplomatie ? La transposition au champ cybernétique du concept stratégique de riposte graduée, initialement destiné au risque nucléaire, est-il envisageable ? Ou encore, faut-il, à l'instar de la France, être prêts à employer l'arme cyber à des fins offensives en opérations extérieures, isolément ou en appui de ses moyens conventionnels, pour en multiplier les effets dans le plus strict respect des normes du droit international public?

Il conviendrait enfin que les deux organisations proposent une définition commune du cyberespace ou du cyberdomaine afin de clarifier la nature profonde du cyber et des activités qui y sont corrélées. Elles pourraient en outre s'accorder sur des critères communs d'évaluation de la capacité d'un État à agir dans le cyberespace, afin d'assurer la cohérence et la complémentarité des efforts déployés, notamment par une coopération dans le domaine de la formation et des exercices mais également par une sensibilisation commune des États à la sécurisation de leurs CIS nationaux.

Améliorations pour la Belgique

Les entreprises belges devraient davantage coopérer pour une meilleure dénonciation des actes de cybercriminalité. Le signalement des cyberincidents devrait être centralisé, singulièrement dans le secteur bancaire afin de permettre une compréhension optimale des problèmes et la construction d'une expertise plus performante. Pour ce faire, il serait judicieux de mettre en place une plateforme nationale pour l'échange des informations entre tous les acteurs de la société belge à propos des menaces, des vulnérabilités et des incidents cyber.

Un des autres défis à relever par la Belgique est celui des technologies financières de pointe qu'il conviendrait de sécuriser par une série de procédés cybersécuritaires pour le plus grand profit de l'utilisateur final, qu'il conviendrait de convaincre de leur pertinence et de leur fiabilité. Il serait par exemple judicieux de développer des méthodes plus performantes de détection des cyberincidents, de meilleurs algorithmes ou des techniques de mégadonnées plus efficaces.

Il serait également opportun de renforcer la coopération interdépartementale, centralisée par le CCB, afin d'ajuster plus rapidement les moyens nationaux disponibles pour contrer les cybermenaces et répondre à nos obligations euro-atlantiques dans les délais impartis.

Tous les services publics et entreprises belges devraient adopter un plan de cybersécurité afin d'augmenter leurs capacités de résilience vis-à-vis des cyberattaques. Au niveau national, l'État pourrait intensifier ses efforts en vue de sensibiliser les internautes quant aux risques liés au numérique et miser davantage sur un recrutement attractif de personnel cyberqualifié afin de pouvoir faire face efficacement à la concurrence du privé.

La Défense a un rôle primordial à jouer dans le domaine de la cyberdéfense. Elle possède en effet une des capacités cybernétiques les plus importantes du pays et contribue ainsi à la sécurité intérieure, en coordination avec le CCB. L'armée constitue, en outre, le dernier rempart des autorités nationales en cas de cyberattaque de grande ampleur contre la Belgique.

La Défense se doit dès lors de renforcer son rôle en matière de cyberdéfense nationale. Tout d'abord, il conviendrait que le service juridique de la Défense, par son expertise dans le droit des conflits armés, contribue davantage, dans le respect de la législation internationale existante, à la mise en place d'un cadre juridique national afin d'être en mesure de répondre aux cyberattaques menées à l'encontre de la Belgique. Ensuite, le service de renseignement de la Défense devrait participer activement à la résolution de la problématique de l'attribution. Enfin, la coopération en matière de formation et de recherche entre l'armée belge d'une part, et le secteur public et privé d'autre part, devrait être renforcée.

En outre, et conformément à ses objectifs stratégiques, il convient que la Défense mette tout en œuvre pour être en mesure de mener des cyberactions offensives à partir de 2020-2025. Ces capacités offensives pourraient, le cas échéant, être utilisées lors des opérations de l'Alliance et renforcer ainsi la contribution militaire de la Belgique sur la scène internationale.

Éléments de bibliographie

La bibliographie est intégrée dans les notes de bas de page. Les ouvrages repris ci-dessous ont été particulièrement utiles à l'auteure pour mener à bien son étude.

Travaux de référence

International

- J. Allen, Ph. M. Breedlove, J. Lindley-French et G. Zambellas, *Future War NATO? From Hybrid War to Hyper War via Cyber War. Supporting Paper of the GLOBSEC NATO Adaptation Initiative*, 2017.
- ITU, *Global Cybersecurity Index (GCI) 2017*.
- J. de Lespinois (sous la dir.), Stratégie du cyberespace, *Stratégique* n°117, 2018.
- V. Joubert et J.-L. Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE », *Hérodote*, n° 152-153, 2014/1.
- McKinsey Global Institute (MGI), *Digital Globalization: The New Era of Global Flows*, mars 2016.
- T. Minarik, R. Jakschis, L. Lindström, (Eds), *10th International Conference on Cyber Conflict. Cycon X: Maximising Effects*, Tallinn, 2018.
- Ponemon Institute, *2017 Cost of Cybercrime Study. Insights on the Security Investments that make a difference*.
- *Symantec Internet Security Threat Report 2018*, vol. 23, mars 2018.
- S. Taillat, A. Cattaruzza et D. Danet (sous la dir.), *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2018.

Belgique

- *Accord de gouvernement de la Belgique*, 9 octobre 2014.
- *Cyber Security Strategy [of] Belgium*, 23 novembre 2012.
- M. Fontaine et M. Benatar, « Cyber-attaques : aperçu du cadre juridique national », *Questions juridiques d'actualité en lien avec la défense*, 2017.
- S.n., « La Cybersécurité : nous sommes tous concernés », [2017] (https://www.febelfin.be/fr/newsletter360/9/table-ronde-complete, consulté le 15 janvier 2019).
- *La Vision stratégique pour la défense*, 29 juin 2016.
- *Stratégie de cybersécurité pour la Défense*, 2014, p. 4 (ACST-Strategy-CyberSecurity-001, Ed 001/Rev 000/30-09-2014).
- J. Van Eyck, *De Belgische cyberdefensie en EU-samenwerking*, ERM, 2018.

Documents UE

- *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé,* février 2013.
- « Directive (UE) 2016/1148 du parlement européen et du conseil du 6 juillet concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information » dans l'Union, *Journal officiel de l'Union européenne*, 19 juillet 2016.
- Communication conjointe au Parlement européen et au Conseil, *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017, p. 3 [JOIN (2017) 450 final].
- Conseil de l'Union européenne, *Cadre d'action de l'UE en matière de cyberdéfense*, Bruxelles, 18 novembre 2014 [15585/14].
- Conseil de l'Union européenne, *Conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique")*, Bruxelles, 19 juin 2017.
- Communication conjointe au Parlement européen et au Conseil. *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Bruxelles, 13 septembre 2017 [JOIN (2017) 450 final].
- *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense*, 2018 (2008/2004 (INI).

Documents OTAN

- *Déclaration du Sommet de Prague diffusée par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord*, 21 novembre 2002.
- *Déclaration du Sommet de Bucarest publiée par les chefs d'État et de gouvernement participant à la réunion du Conseil e l'Atlantique Nord tenue à Bucarest le 3 avril 2008.*
- *Concept stratégique pour la défense et la sécurité des membres de l'Organisation du Traité de l'Atlantique Nord adopté par les chefs d'État et de gouvernement à Lisbonne*, 19 novembre 2010.
- *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 les 4 et 5 septembre 2014*, 7 septembre 2014.
- *Communiqué du Sommet de Varsovie publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Varsovie les 8 et 9 juillet 2016*.

Institut Royal Supérieur de Défense
Centre d'Etudes de Sécurité et Défense
30 Avenue de la Renaissance
1000 Bruxelles