Université de Montréal

La contribution des dynamiques internationales formelles au renforcement de la cybersécurité canadienne

par Carolle Vodouhe

Faculté de droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de maîtrise en droit (LL.M.)
option droit des technologies de l'information

Mai 2015

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

La contribution des dynamiques internationales formelles au renforcement de la cybersécurité canadienne

présenté par
Carolle Vodouhe

a été évalué par un jury composé des personnes suivantes :

Nicolas W. Vermeys

Directeur de recherche

Karim Benyekhlef

Membre du jury

Amissi M. Manirabona

Membre du jury

RÉSUMÉ

La cybersécurité représente un enjeu important pour les services en charge de la sécurité canadienne à l'ère de l'expansion des Menaces Persistantes Avancées (MSP ou cybercrimes de type 1). Ces crimes se déroulent essentiellement dans le cyberespace, ce qui implique l'adoption de mesures spécifiques adéquates à l'environnement numérique, notamment à l'épreuve de son ubiquité. Le gouvernement canadien a pour sa part publié certaines mesures de défense passive et active dont la plus connue est la stratégie canadienne de cybersécurité. Puisque le cyberespace n'est pas limité territorialement, l'autorité canadienne a conclu plusieurs partenariats internationaux d'où ressortent des mesures bilatérales et multilatérales de protection et de renforcement de la cybersécurité. Toutefois, ces diverses mesures nationales et internationales ne tracent pas de cadre légal précisant la nature et le régime juridique des MSP; précisions sans lesquelles l'adoption de règles au plan national serait improductive. Considérant que l'espace numérique est international, il appelle la mise en place de mesures applicables à l'échelle universelle. Or, au plan international, il n'existe aucun texte à valeur légale spécifique à l'espèce. Ainsi, à la question de savoir, quels textes légaux pourraient s'appliquer, il s'est avéré que le *jus ad bellum* et la Convention européenne contre le cybercrime (Convention de Budapest) apportaient d'incontournables éléments de réponse. D'une part, le *jus ad bellum* permet de définir la catégorie d'acte dans laquelle peuvent être rangées les MSP, et d'autre part, la Convention de Budapest permet de définir les infractions informatiques commises par les différents acteurs en cause, les procédures d'investigation appropriées et les mécanismes utiles à la coopération internationale. Bien que les éléments ressortis de ces ententes internationales soient utiles à l'adoption d'un corps de règles internationales uniformes, les intérêts étatiques divergents constituent des obstacles de taille.

Mots-clés : **Canada, convention de Budapest, cybersécurité, cybercriminalité, infrastructures critiques, cybercrimes de type 1, MSP.**

ABSTRACT

Cyber security is an important issue for services in charge of Canadian security in the era of the expansion of Advanced Persistent Threats (MSP cybercrimes or type 1). These crimes are conducted primarily in cyberspace, which implies the adoption of specific measures appropriate to the digital environment, including the test of its ubiquity. The Canadian government, for its part published some passive and active defense measures which the best known is the Canadian cyber security strategy. Since cyberspace is not limited territorially Canadian authority has signed several international partnerships which emerge from bilateral and multilateral measures for the protection and strengthening cybersecurity. However, such national and international measures do not draw legal framework specifying the nature and the legal regime of MSP; information without which the adoption of rules seems counterproductive. Whereas the digital space is international, it calls the implementation measures for universal scale. However, internationally, there is no rule with specific legal value. Thus, the question is what legal texts could be applied? It turned out that the *jus ad bellum* and the European Convention against Cybercrime (Budapest Convention) brought the inevitable answer. First, *jus ad bellum* to define the category of act in which can be stored MSPs, and secondly, the Budapest Convention allows defining computer offenses committed by different actors involved, appropriate investigative procedures and useful mechanisms for international cooperation. Although the elements emerged from these international agreements be useful to the adoption of a set of uniform rules, divergent state interests are major obstacles.

Keywords : **Canada, Budapest Convention, cybersecurity, cybercriminality, critical infrastructure, cybercrimes type 1, MSP.**

TABLE DES MATIÈRES

LISTE DES SIGLES ET ABRÉVIATIONS

Akron Intell. Prop. J.: Akron Intellectual Property Journal

Berkeley Tech. L.J.: Berkeley Technology Law Journal

B.F.L.R.: Banking & Finance Law Review

Brook. J. Corp. Fin. &Com. L.: Brooklyn Journal of Corporate, Financial and Commercial law

CAI : Commission d'accès à l'information

CAF: Cour d'Appel Fédérale

Cal. L. Rev.: California Law Review

Can.-U.S. L.J.: Canada-United States Law Journal

CAN/CSA: Association canadienne de normalisation/Canadian Standard Association

Can. J.L. & Tech: Canadian Journal of Law and Technology

CISAC: Center for International Security and Cooperation

CNIL : Commission Nationale de l'Informatique et des Libertés

CSTC : Centre de la Sécurité des Télécommunications du Canada

DCS : Distributed Control System

D.T.E. : Droit du travail express

Duke J. Comp. & Int'l L.: Duke Journal Comparative and International Law

GPS: Global Positioning System

GRC: Gendarmerie Royale du Canada

GSM: Global System for Mobile Communications

Hastings L.J.: Hastings Law Journal

Hous. L. Rev.: Houston Law Review

ICS: Industrial Control Systems

IEEE: Institute of Electrical and Electronic Engineers

J.E. : Jurisprudence express

J. Pol. Anal. Manage.: Journal of Policy Analysis and Management

L.C. : Lois du Canada

L.R.C. : Lois révisés du Canada

L.G.D.J. : Librairie Générale de Droit et de Jurisprudence

McGill L.J.: McGill Law Journal

Mich. L. Rev.: Michigan Law Review

Mich. St. J. Int'l L: Michigan State University College of Law Journal of International Law

MSP: Menaces Persistantes Avancées

OCDE : Organisation de Coopération et de Développement Économique

OÉA: Organisation des États Américains

OIPC: Office of the Information and Privacy Commissioner

R.C.S. : Recueil des arrêts de la Cour Suprême

R.D.U.S. : Revue de droit de l'Université de Sherbrooke

R.J.Q. : Revue juridique du Québec

R.J.T. : Revue juridique Thémis

R.L. : Revue Légale

RSI : Responsable de la Sécurité Informationnelle

SCADA : Supervisory Control And Data Acquisition

S. Cal. Interdisc. L.J.: South California Interdisciplinary Law Journal

SBNL: Security Breach Notification Laws

SCRS: Service Canadien du Renseignement de Sécurité

Vand. J. Transnat'l L.: Vanderbilt Journal Transnational Law

Vill. L. Rev.: Villanova Law Review

W. New Eng. L.Rev.: Western New England Law Review

À ma famille, qui m'a enseignée que la persévérance et la prière sont la clé de la réussite.

REMERCIEMENTS

Tout d'abord merci à mon directeur de recherche, le professeur Nicolas Vermeys, pour l'enthousiasme manifesté à l'égard de mon projet, pour tous vos commentaires et suggestions ainsi que pour votre disponibilité. Avoir l'occasion de vous côtoyer pendant ce projet a été un honneur pour moi.

Je tiens également à remercier, et je ne le ferai jamais assez, mes parents pour leur indéfectible soutien.

« *Nos systèmes sont des cibles attrayantes pour les services militaires et du renseignement étrangers ainsi que pour les réseaux criminels et terroristes*. »[1]

Introduction

La cybersécurité est un enjeu contemporain qui est au cœur des activités de sécurité intérieure de tout pays. Ce domaine a considérablement crût avec l'intensification des échanges se produisant dans le cyberespace, l'augmentation du flux d'informations inestimable et le nombre considérable des exploitants de ce système.

La cybersécurité, en tant que partie intrinsèque de la sécurité intérieure d'un gouvernement fait appel à une dynamique institutionnelle qui implique de nombreux acteurs gouvernementaux et du secteur privé. La communauté internationale est également comprise dans la dynamique, car le cyberespace n'est pas limité territorialement. Pour épouser les mots de la doctrine, il est caractérisé par son ubiquité. Tout ce qui se déroule dans l'internet ouvert est accessible dans le monde entier.

Cet environnement n'est pas limité par des frontières physiques et requiert donc la mise en œuvre de nouvelles procédures de gestion des échanges et de régulation des activités qui s'y déroulent. Ces activités sont diverses, allant du légal à l'illégal[2].

Ainsi, le crime se meut pour intégrer une dimension informatique dans sa commission, il peut aussi incarner un pur produit de l'environnement cybernétique. Pour illustrer, selon David Décary-Hétu, la fraude informatique par exemple n'est qu'une extension, une

[1] MINISTÈRE DE LA SÉCURITÉ PUBLIQUE DU CANADA, Stratégie de cybersécurité du Canada. Renforcer le Canada et accroître sa prospérité, 2010 [Stratégie canadienne], p. 1.

[2] COMMISSARIAT DU CENTRE DE LA SECURITE DES TELECOMMUNICATIONS, *Rapport annuel 2012-2013*, Juin 2013, à la page 7, le commissaire en fonction alors, Robert Décary affirmait : «On ne peut plus parler de sécurité sans évoquer les cybermenaces ».

évolution de la fraude classique[3], punit par l'article 380 du *Code Criminel du Canada*[4] (*Code Criminel*); alors que le piratage est né de l'informatique. Selon certains auteurs, la criminalité informatique est fléau numérique[5] qui s'impose comme une problématique importante de la cybersécurité. A ce titre, elle mobilise d'importantes ressources financières. En ce sens, elle amène les États-Unis à investir plus de 25 milliards de dollars US[6] par année dans la défense numérique et l'autorité canadienne a injecté quant à elle près de 1.4 milliards de dollars en 2012[7] dans la prévention contre les cybercrimes majeurs.

Ces dépenses sont justifiées par l'ampleur des cybermenaces qui planent sur la sécurité des personnes et des biens. La *Security and defence agenda* recense 4 activités illégales au nombre des cybermenaces les plus coûteuses pour les administrations publiques. Ce

[3]David DÉCARY-HÉTU, *La cybercriminalité*, Les mots de l'économie numérique, Chaire L. R. Wilson, Université de Montréal, 17 Mars 2015, disponible en ligne : http://www.chairelrwilson.ca/fr/calendrier/ (consulté le 08 Avril 2015).

[4] L.R.C. (1985), c. C-46, art 380.

[5] Voir en ligne : Lorenzo ALTESE, « Cybercriminalité : un fléau en hausse en France ! », **(**14 Décembre 2014**)**, disponible en ligne : http://blog.economie-numerique.net/2012/12/14/cybercriminalite-un-fleau-en-hausse-en-france/ (consulté le 5 Avril 2014) ou, Gilbert KALLERBORN, « Cybercriminalité: les forces de l'ordre en formation continue », **(**21 Janvier 2014**)**, disponible en ligne : http://www.01net.com/editorial/612428/cybercriminalite-les-forces-de-lordre-en-formation-continue/ (consultés le 18 Août 2014). Il convient toutefois de tempérer ces données qui sont la plupart du temps majorée par les sociétés de cybersécurité. Voir à ce propos D. DÉCARY-HÉTU, préc., note 3.

[6]Le coût se rapporte essentiellement à la lutte contre le cyberespionnage étatique et représente les chiffres avancés par les États-Unis. Voir Danilo D'ELIA, « La guerre économique à l'ère du cyberespace », **(**2014**)** 1-2 *Hérodote* 240, 240-260, disponible en ligne : http://www.cairn.info/zen.php?ID_ARTICLE=HER_152_0240 (consulté le 10 Septembre 2014); Ronald DEIBERT, *Black Code : inside the battle of the cyberespace*, 1st, Toronto, McClelland & Stewart, 2013, p. 144 : « Cyber crime has become one of the world's largest growth businesses. (Estimated vary, and the self-interest of threat inflation cannot be ignored, but the National Security Agency's General Keith Alexander has estimated that American companies lose around $250 billion from IP theft, and that internationally cyber crime causes $114 billion in losses. The computer security company one thing in clear: it's large). »

[7] GROUPE CGI INC., « La cybersécurité, une source de préoccupation constante pour les Canadiens : les clients tirent profit de l'expertise locale et mondiale de CGI pour atténuer leur niveau de risque », Communiqué de presse, 2 avril 2013, Ottawa, disponible en ligne http://www.cgi.com/fr/Cybersecurite-preoccupation-expertise-locale-mondiale-CGI-attenuer-niveau-risque(consulté le 5 Décembre 2014).

sont le cyberhacktivisme (ou la guerre de salon)[8], le *Cloud hacking*[9], le *Mobile and tablet hacking*[10], et les *Advanced persistants threats* (Menaces persistantes avancées (MSP))[11], ou cybercrimes de type 1[12]). C'est sur ces derniers types de menaces que nous concentrerons notre analyse dans le cadre de la présente étude.

La particularité des MSP se rapporte à l'incidence directe qu'ils ont sur les infrastructures critiques d'un pays, car la menace porte sur l'entité étatique et vise directement, ou de façon détournée, la déstabilisation d'un État, que ce soit dans le but de lui infliger des pertes économiques[13], ou des pertes en vies humaines[14]. M. Schmitt affirme à cet effet:

> « In fact, malevolent states, cyberterrorists, or malicious hackers will likely exploit cyberspace to strike at global critical infrastructure and other essential cyberassets. The ensuing consequences of such operations could range from the disruption of government functions and economic loss to massive physical destruction and widespread death. »[15]

De façon sommaire, une MSP consiste en l'utilisation d'un ou de plusieurs maliciels afin d'interrompre, de détruire ou de corrompre une part ou tout un système informatique essentiel au bon fonctionnement d'une partie ou de tout l'engrenage étatique. L'attaque

---

[8] Benoît GAGNON, *Le cyberterrorisme*, Interview par Jean-François LISÉE, CERIUM, Université de Montréal, 20 Novembre 2009, Montréal, disponible en ligne https://www.youtube.com/watch?v=4rA9AzSEHXM (consulté le 7 Janvier 2015).

[9] SECURITY & DEFENCE AGENDA*, Cyber-security: The vexed question of global rules An independent report on cyber-preparedness around the world*, Brussels, Février 2012, [SDA], p. 41, disponible en ligne: www.securitydefenceagenda.org (consulté le 20 Janvier 2015).

[10] *Id.*, p. 41-42.

[11] SERVICE CANADIEN DU RENSEIGNEMENT DE SECURITE, *Études hors-séries, Évaluation des cybermenaces pesant contre les infrastructures, Rapport préparé pour le Service Canadien de Renseignement de Sécurité*, 2012, Angela GENDRON et Martin RUDNER, [Études hors-séries], disponible en ligne https://www.csis-scrs.gc.ca/pblctns/ccsnlpprs/20121001_ccsnlpprs-fr.php (consulté le 13 Décembre 2014).

[12] Reese NGUYEN, « Navigating Jus Ad Bellum in the Age of Cyber Warfare », **(**2013**)** 101 *Cal. L. Rev.* 1079, 1087.

[13] Études hors-séries, préc., note 11, p. 8-17.

[14] J. LEWIS (dir), *Cyber security Turning National solutions into international cooperation*, Washington, the CSIS Press, Significant issues series, 2003, p. xiv à xv.

[15] Michael SCHMITT, « Cyberspace and international law: the penumbral mist of uncertainty », **(**2012-2013**)**, 126 *Harv. L. Rev. F.* 176, 176.

peut être portée à l'un de ses secteurs vitaux comme l'énergie, par exemple[16]. Lorsque les effets d'une MSP peuvent être perceptibles[17] par les dégâts physiques qu'elle cause, elle peut être qualifiée de dynamique au contraire d'une MSP dont les manifestations ne sont pas flagrantes. Dans ce cas-là, il s'agira alors d'une MSP passive car elle se manifeste par une simple intrusion dans un système informatique dans le but de voler de l'information. Plusieurs manifestations de MSP, encore appelées cyberattaques informatiques, ont consacré la naissance de deux néologismes au cours de ces dernières années, le cyberterrorisme et le cyberespionnage étatique.

Le cyberterrorisme est sommairement entendu comme l'utilisation de l'internet par des terroristes [18] . Il découle du terrorisme international classique et son existence est étroitement liée à celle de l'internet. Ce dernier représente à la fois l'outil[19] et la cible[20] de ses acteurs[21]. La menace que représente le cyberterrorisme pour la stabilité d'un État et la paix globale est équivalente au terrorisme classique mais, au vu des outils utilisés, ses

[16] Études hors-séries, note 11, à la p. 14. Le gouvernement canadien fonde son fonctionnement sur dix infrastructures critiques :

> «· Énergie et services publics : Ressources naturelles Canada
> · Technologies de l'information et de la communication : Industrie Canada
> · Finances : Finances Canada
> · Alimentation : Agriculture et Agroalimentaire Canada
> · Santé : Agence de la santé publique du Canada
> · Secteur manufacturier : Industrie Canada, Défense nationale
> · Sécurité : Sécurité publique Canada
> · Transport : Transports Canada
> · Eau : Environnement Canada ».

[17] Ici, la perception doit également être entendue comme la constatation d'une manipulation dans un système informatique ou la simple intrusion dans celui-ci.

[18]Voir généralement COUNCIL OF EUROPE, *Cyberterrorism-the use of the internet for terrorist purposes*, 1st, Strasbourg, Council of Europe publishing, 2007 [Cyberterrorism].

[19]Voir généralement Susan W. BRENNER and Marc D. GOODMAN, « In defense of cyberterrorism: an argument for anticipating cyber-attacks », **(**2002**)** 1*U. Ill. J.L. Tech. &Pol'y* 1.

[20] *Id.*, l'internet est une cible des assaillants lorsqu'ils visent la destruction ou la corruption des connexions d'un réseau internet utile au fonctionnement interne d'un État.

[21] Mohammad IQBAL, « Defining Cyberterrorism », **(**2003-2004**)** 22 *J. Marshall J. Computer & Info. L.* 397, 398.

effets sont estimés plus rapides et illimités territorialement[22]. A ce propos, Kelly A. Gable écrit: « without ever having to build a bomb or sacrifice themselves, cyberterrorists can bring down the critical infrastructure of an entire state, disrupt the global economy, and install fear and chaos among billions of people[23] ». En avril 2015, par exemple, des pirates de l'État Islamique ont causé d'importants dommages à la chaîne TV5Monde en prenant le contrôle de sa plateforme numérique. Selon le Premier ministre français, Manuel Valls, cet acte était une « atteinte inacceptable à la liberté d'information et d'expression »[24].

D'égale ampleur, le cyberespionnage étatique est le fait d'un État qui opère un vol d'informations confidentielles dans les bases de données d'une entité homologue afin d'en tirer un avantage qui peut être économique ou militaire[25] au détriment de l'État visé.

L'un des problèmes qui ressort en général des investigations sur des cas de cybercrimes de type 1 se rapporte à la difficulté de retracer une attaque contre les structures d'un réseau, surtout lorsque cette attaque vient d'un État, lequel peut utiliser des intermédiaires[26] pour atteindre son objectif[27]. Cette suite d'intermédiaires est un obstacle à

[22] Gabriel WEIMANN, *www.terror.net. How Modern Terrorism Uses the Internet*, Washington DC, Special Report, United States Institute of Peace Press, 2006, p. 9.

[23] Kelly GABLE, « Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent », **(**2010**)** 43 *Vand. J. Transnat'l L.* 17, 19, disponible en ligne: www.nsf.gov/news/special-reports/nsf-net/textonly/80s.jsp(consulté le 18 Mars 2014).

[24] LeMonde.fr, « TV5 Monde piraté par un groupe djihadiste », 9 Avril 2015, disponible en ligne http://www.lemonde.fr/pixels/article/2015/04/09/les-sites-de-tv5-monde-detournes-par-un-groupe-islamiste_4612099_4408996.html (consulté le 9 Avril 2015).

[25]Stratégie canadienne, note 1, p. 5.

[26] Ces intermédiaires peuvent être de toute nature. Dans la plupart des cas de cyberattaques de type 1, ce sont des fournisseurs de botnets qui sont sollicités. Voir Jennifer A. CHANDLER, « Security in cyberespace : Combatting Distributed Denial of Service Attacks », **(**2003-2004**)** 1 *Revue de droit et technologie de l'université d'Ottawa* 2, 233-375 ; B. GAGNON, *Le cyberterrorisme*, préc., note 8.

[27]INFORMATION WARFARE MONITOR, *Tracking GhostNet: Investigating a cyber espionage network*, Canada, 2009, p. 7 [Tracking Ghosnet], disponible en ligne : http://fr.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network (consulté le 14 Janvier 2014).

l'attribution de l'acte[28]. Pour l'illustrer, la Chine a été présumée auteur[29] de plusieurs cas de cyberattaques[30] sans que ces allégations ne puissent être prouvées[31].

Ainsi, le problème de l'attribution [32] représente une impasse à laquelle aboutissent immanquablement les enquêtes sur les cyberattaques, car tracer l'origine d'une cyberattaque se révèle une tâche fastidieuse et improductive. Les multiples interconnexions sont un labyrinthe miroitant des pistes possibles qui ne sont que des leurres [33]. De plus, les indices disséminés sur plusieurs territoires empêchent une investigation de fond due au manque évident d'informations logiques et concordantes.

[28]Louis J. ZIVOT, « The Transnational Dimension of Cyber Crime and Terrorism », **(**2001-2002) 34 *N.Y.U Journal of International Law and Politics* 475, 507, disponible en ligne : http://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/nyuilp34&page=505#515 (consulté le 6 Mars 2013).

[29] Nathan THORNBURGH, « The Invasion of the Chinese Cyberspies », 29 Août 2005, TIME, disponible en ligne : http://content.time.com/time/magazine/article/0,9171,1098961-1,00.html (consulté le 10 Avril 2014); DELOITTE, *Cyber Espionage The harsh reality of advanced security threats*, Center for Security & Privacy Solutions, 2011, disponible en ligne : http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_cyber_espionage_07292011.pdf (consulté le 16 Octobre 2014); Mandiant, *APT1 Exposing One of China's Cyber Espionage Units,* 2004, disponible en ligne : http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (consulté le 13 Avril 2014) [Rapport Mandiant]; Daniel VENTRE, *Une analyse du rapport Mandiant*, Chaire de cyberdéfense et de cybersécurité, Juillet 2013, disponible en ligne : http://www.chaire-cyber.fr/IMG/pdf/article_4_1_-_chaire_cyberdefense.pdf (consulté le 10 Juillet 2014).

[30] En 2011 par exemple, le Secrétariat du Conseil du Trésor fut victime d'un cyberespionnage dont l'attribution à l'autorité chinoise n'a pu qu'être alléguée. Des fonctionnaires interviewés «ont souligné qu'il était impossible de déterminer si les auteurs de cette attaque étaient chinois ou si, d'une autre nationalité, ils avaient simplement utilisé des serveurs basés dans le pays communiste » et, selon la chaîne CTV, « il s'agit de pirates employés par le gouvernement chinois. ». L'épineux problème de l'attribution est d'ailleurs soulevé : «L'espionnage en provenance de Chine est devenu un problème majeur pour le Canada», a dit à CTV un fonctionnaire «haut placé» sous le couvert de l'anonymat. ». Voir Clément SABOURIN, « Ottawa victime d'une cyberattaque venant de Chine », 16 février 2011, La Presse Canadienne, Ottawa, disponible en ligne : http://www.lapresse.ca/actualites/politique/politique-canadienne/201102/16/01-4371042-ottawa-victime-dune-cyberattaque-venant-de-chine.php (consulté le 17 Novembre 2014).

[31] Le rapport Mandiant montre plusieurs indices qui orientent vers l'implication de la Chine mais aucune ne constitue de réelles preuves. Rapport Mandiant, préc., note 29.

[32] Reese NGUYEN, préc., note 12, p. 1104-1106.

[33]Hypponen MIKKO, « Fending off attacks in cyberspace, the global nature of cyberwarfare », 29 Mai 2009, NYTimes.com, cité par Georg KERSCHICHNIG, *Cyberthreats and international law*, 1st ed., Hague, Eleven International Publishing, 2012, p. 12.

C'est en ce sens qu'une défense passive[34] et active[35] contre ces phénomènes se révèle une option sécuritaire primordiale.

Comme nous l'avions mentionné, la cybersécurité, en tant que mécanismes voués à la sécurité du cyberespace, se veut par essence une sécurisation à l'international[36]. Ceci s'explique par l'ubiquité de l'environnement numérique, les origines des cyberattaques multiples et éloignées géographiquement, les répercussions des cyberattaques sur la paix et la stabilité internationale et, surtout, l'implication des acteurs étatiques. De plus, l'exigence d'une sécurité internationale est justifiée par la vitalité des cibles que visent les MSP comme le cyberespionnage étatique et le cyberterrorisme dans la société et dans le développement d'une nation. Ce sont, en effet, les infrastructures critiques d'un pays qui seront ciblées par les contrevenants[37]. Du fait de leurs composantes, celles-ci incarnent le cœur de l'activité étatique et/ou économique mais dénotent de grandes vulnérabilités, que ce soit au niveau des interconnexions[38] qui existent entre elles ou du rôle qu'elles jouent

[34] Seymour Goodman écrit : « passive defense is essentially target hardening. It consists largely of the internal use of various technologies and products […] and procedures […] to protect the information technology (IT) assets owned by an individual or organization. Some forms of passive defense may be dynamic (e.g., stopping an attack in progress). By definition, however, passive defense does not impose serious risks or penalties on the attacker. With only passive defensive measures, the attacker is free to continue assault the target until he either succeeds or gets frustrated and looks elsewhere. » Voir Seymour GOODMAN, « Toward a treaty-based international regime on cyber crime and terrorism » dans J. Lewis, préc., note 14, p. 66.

[35] *Id.*, toujours selon Seymour Goodman, la défense active comporte plusieurs aspects : - la sanction du criminel, - l'arrêt de l'attaque en cours, - les mécanismes d'enquête et de poursuite, - les mécanismes légaux. Ce type de défense impose de sérieux risques aux attaquants et les expose à des sanctions. Ces risques ou sanctions peuvent être : « identification and exposure, stopping an attack in progress, investigation and prosecution, or preemptive or counterattacks of various sorts »; M. CASTLE définit la défense active en ces termes : « An active defense in cyberspace seeks to identify and even neutralize threats before they materialize ». Michael CASTLE, « International and Canadian Law Rules Applicable to Cyber Attacks by State and Non-State Actors » **(**Juin 2012**)** 10 *Can. J. L. & Tech.* 89 1, 19 [note 10].

[36] Vytautas BUTRIMAS, Conseiller du chef exécutif de la cybersécurité en Lituanie, cité dans SDA, préc., note 9, p. 18.

[37] Theodore C. THEOFRASTOUS, « Security and the economy: the North American computer and communication infrastructure », **(**Avril 2003**)** 29 *Can.-U.S. L.J.* 225 1, 5.

[38] Ces interconnexions s'étendent entre les différentes infrastructures à des degrés divers et parfois inégaux. La dépendance peut être due à un lien physique, géographique ou cybernétique. Il y a donc interdépendance « lorsque les producteurs et les fournisseurs de produits et de services, tant au sein qu'entre les secteurs des infrastructures essentielles, deviennent dépendants l'un de l'autre, […] » Etudes hors-séries, préc., note 11, p. 14; L'interconnexion peut résulter également d'un rapport réseau-service ou réseau-support. Au niveau des infrastructures énergétique par exemple, l'interconnexion s'étend à l'international. Voir Jean-Pierre

dans le développement du pays, ou encore du renseignement qu'elles véhiculent et/ou produisent.

Considérant ces risques et les effets déjà connus de certains cybercrimes de type 1, certaines organisations internationales ont publié des directives de cybersécurité [39] applicables au sein des différents États-membres[40]. Plusieurs gouvernements se sont également empressés d'élaborer et de publier des stratégies nationales de cybersécurité[41] destinées à placer des balises contre ces MSP[42]. Ainsi, à l'instar de la publication de sa

---

GALLAND, « Critique de la notion d'infrastructure critique », **(**2010**)** 3 *Flux* 81 6-18; Robert RADVANOVSKY et Allan MCDOUGALL, *Critical infrastructure Homeland Security and Emergency preparedness*, 2nde, New York, CRS press, 2010, p. 3.

[39]L'Organisation de Coopération et de Développement Économique (OCDE) a, par exemple, publié en juillet 2002, des directives de cybersécurité que chaque Etat-membre peut mettre en place pour prévenir les cyberattaques. CONSEIL DE L'ORGANISATION POUR LE COMMERCE ET LE DÉVELOPPEMENT ÉCONOMIQUE, *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information. Vers une culture de la sécurité*, 1037ème session, Juillet 2002.

[40] *Id*., à la p. 14:

> « Recognising that there is a common interest in promoting the security of information systems and networks by means of a culture of security that fosters international co-ordination and co-operation to meet the challenges posed by the potential harm from security failures to national economies, international trade and participation in social, cultural and political life. » [Nous soulignons].

[41] Pour Ronald Deibert, c'est la « cybersécurité distribuée » qui correspond à l'idéal d'une garantie efficace de lutte. Il affirme, partant du constat de l'artificialité du cyberespace, que la dépendance de l'Homme à l'internet est réciproque pour montrer que la meilleure stratégie de défense ne peut émaner que de lui. L'individu, dans son rôle de principal intervenant est considéré en tant que civil mais aussi professionnel et est appuyé par les gouvernements et le secteur privé au sein d'un système transnational. Il affirme précisément ceci:

> « Governments, NGOs, armed forces, law enforcement and intelligent agencies, private sector companies, programmers, technologists, and average users must all play vital and interdependent roles as stewards of cyberspace. Concentrating governance of cyberspace in a single global body, whether at the UN or elsewhere, makes no sense. The only type of security that functions in an open, decentralized networked is distributed security ».

L'idée d'une cyberstratégie distribuée qui voudrait que l'ordre émane du chaos et qu'émerge ainsi des mini-pôles de contrôle réparties entre les différents acteurs semble être une alternative intéressante à l'adoption de normes de sécurité restreintes territorialement. Mais comment un tel procédé peut-il être mis en œuvre ? Sous-tendant l'avènement d'un chaos, il ne serait clairement pas possible d'initier une destruction de l'internet dans le monde actuel. Toutefois, souligner l'importance de l'adoption de normes transnationales ramène la réflexion vers la nécessité d'une normativité internationale. Le caractère international des multiples conventions interétatiques et régionales sont adéquates à une lutte efficace puisqu'elles épousent les spécificités du cyberespace. R. DEIBERT, préc., note 6, p. 239.

[42] Les États-Unis sont considérés comme les pionniers dans l'élaboration de cyberstratégies de défense. Ainsi, selon un tableau exhaustif, Benoit Dupont dresse un résumé de l'évolution des adoptions de stratégies

stratégie de cybersécurité[43], le gouvernement canadien a établi plusieurs ententes internationales auxquelles participent activement ses services de renseignements. Parmi ces multiples coopérations[44], le pays s'est allié avec les États-Unis et avec les pays représentant les Five Eyes (cette organisation sera abordée *infra*) avec lesquels il effectue des échanges d'informations de sécurité dans le but de renforcer leurs infrastructures communes. Cependant, aucune de ces alliances ne porte sur un encadrement législatif des cybercrimes de type 1[45] qui pourrait permettre la mise en place d'une cybersécurité globale efficace.

Nous sommes d'avis que, sans dispositions légales internationales encadrant ces infractions d'envergure, l'application d'une cybersécurité au plan national ne serait ni effective ni complète. A cet égard, il est donc apparu important, dans une logique de contribution au renforcement de la cybersécurité canadienne, d'étudier au plan international les textes juridiques qui pourraient indiquer les voies à suivre pour une

---

numériques au niveau de l'Occident et des Amériques. Voir : Benoit DUPONT, « The proliferation of cybersecurity strategies and their implications for privacy », dans Esther MITJANS et Karim BENYEKLEFF, *Circulation internationale de l'information et sécurité*, 1ère éd., Montréal, Éditions Thémis, 2013, p.67.

[43]Stratégie canadienne, préc., note 1.

[44] Le pays fait également partie de l'Organisation des États Américains (ci-après OÉA), l'Organisation pour le Commerce et le Développement Économique (ci-après OCDE) et le Groupe des 8 (ci-après G-8) dont les stratégies de défense numérique garantissent respectivement la résilience des infrastructures critiques communes, un commerce électronique sûr et un guide de mesures de cybersécurité à mettre en place au plan national. Concernant l'OEA, le Ministère des affaires étrangères canadien a établi avec l'organisation une collaboration en vue d'accroître la résilience des infrastructures critiques. Voir en ligne AFFAIRES ETRANGERES ET DEVELOPPEMENT CANADA, Canada et l'Organisation des Etats-Américains, disponible en ligne : http://www.international.gc.ca/american_states-etats_americains/oas-oea/oas-oae.aspx?lang=fra ou ORGANIZATION OF AMERICAN STATES, disponible en ligne : http://www.oas.org/en/sms/cicte/programs_cyber.asp (consultés le 10 Mai 2014). Avec le G8, le gouvernement a mis en place un ensemble de mesures pour permettre un échange continu d'information entre les différents membres ainsi qu'un mécanisme d'entraide internationale en 2000. Voir en ligne http://www.cybercrime.gov/principles.htm (consulté le 17 Septembre 2014). Pour plus d'informations sur l'OCDE, voir OCDE, préc., note 39.

[45]Pottengal MUKUNDAN, « Laying the foundation of a cyber-secure world » dans J. LEWIS, préc., note 14, p. 35: C'est afin d'apporter des éléments de réponse à ce vide juridique qu'une communauté d'experts s'est réuni pour rédiger le Manuel de Tallinn. Celui-ci trace un cadre de définition de ce que représente les cyberattaques étatiques au regard du droit international humanitaire. Voir Michael SCHMITT (dir.), *Tallinn manual on the international law applicable to cyber warfare*, 2013, [Tallinn], disponible en ligne http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=0/1803379#search (consulté le 14 Décembre 2014).

possible régulation de la lutte contre les MSP à la même échelle. Il importe alors de répondre à la problématique suivante : de quel cadre normatif international le Canada peut-il s'inspirer pour renforcer sa cybersécurité?

Dans le registre de la cybercriminalité informatique, le texte international ayant reçu un grand nombre de signatures est la Convention sur la cybercriminalité adopté par le Conseil de l'Europe en 2001[46] (ci-après Convention de Budapest). Le Canada en est d'ailleurs l'un des signataires[47] mais ne l'a cependant pas ratifié, contrairement à la plupart de ses alliés[48]. Bien qu'elle ait une vocation exclusivement pénale encadrant seulement les cybercrimes de type 2[49], est-il possible que certaines de ses mesures puissent s'appliquer aux MSP[50]? En quoi la Convention de Budapest peut-elle servir de fondement à un futur cadre légal international définissant la nature et le régime juridique de ces menaces? La Convention peut-elle contribuer au renforcement du cadre juridique de la cybersécurité au Canada? Par ailleurs, le *jus ad bellum*[51] qui régit les relations entre États au plan international peut-il s'appliquer aux MSP?

---

[46] Convention sur la cybercriminalité, 23 Novembre 2001, STE n°185 (entrée en vigueur le 1er Juillet 2004), disponible en ligne : http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm (consulté le 10 Août 2014) [Convention de Budapest].

[47] Les États-Unis l'ont signé le 23 Novembre 2001 et l'ont ratifié le 29 Septembre 2006. Le Canada l'a signé à la même date mais ne l'a pas encore ratifié. Il est possible d'en déduire la place de la cybersécurité dans la dynamique gouvernementale.

[48] Les États-Unis en l'occurrence ont pris une part très active dans l'élaboration de cette convention. Amalie Weber remarque d'ailleurs la grande similarité qui existe entre les infractions dressées dans la Convention Européenne et les textes de cybersécurité américaine. Amalie WEBER, « The council of Europe's convention on cybercrime », **(**2003**)** 18 *Berkeley Tech. L.J.* 425, 435-439.

[49] Pour marquer la différence entre les cybercrimes de type 1, nous désignons par cybercrimes de type 2 les crimes informatiques de moindres envergures comme la fraude informatique ou le vol d'identité. Ces derniers ne visent pas la destruction ou l'altération des actifs d'un État.

[50] Selon plusieurs auteurs, la Convention européenne est la réponse la plus sûre à la répression du cybercrime. Victor PLATT, « Still the fire-proof house? An analysis of Canada's cyber security strategy », **(**Hiver 2011-12**)** *International Journal* 154, 159.

[51] Le *jus ad bellum* désigne : « the international law governing the resort to force by States as an instrument of their national policy ». Voir Tallinn, préc., note 45, p. 4; R. NGUYEN, préc., note 12, p. 1112-1113; Jay P. KESAN and Carol M. HAYES, « Mitigative counterstriking: self-defense and deterrence in cyberspace » **(**2011-2012**)** 25 *Harv. J. L. & Tech.* 429, p. 524-525.

Comme la Convention de Budapest est le seul texte à valeur internationale et qu'il s'adresse spécifiquement aux crimes informatiques, nous pensons qu'il est indispensable au renforcement de la cybersécurité canadienne.

Pour démontrer son importance dans cette dynamique, il faut considérer au premier plan que l'inexistence au plan international de qualification juridique des MSP oblige, dans le cadre d'une étude, à ne prendre en compte que des exemples de leurs manifestations pour avoir un aperçu du danger qu'elles représentent pour les États. Ensuite, l'importance des cibles visées par ce type d'acte exacerbe le danger que représente une cyberattaque contre leur bon fonctionnement. Les vulnérabilités issues de leur interdépendance est un facteur des plus à risque puisqu'elle lie plusieurs pays en cas de cyberattaque[52]. Les effets s'étalent donc sur plusieurs États et la seule protection au plan national ne permet pas de déployer des mécanismes transfrontières de contre-offensive, surtout s'il n'existe pas de partenariats entre les pays touchés. La Convention de Budapest vient par exemple dresser un cadre formel de coopération internationale dans les investigations sur les cybercrimes informatiques. La cybersécurité se révèle donc être aussi importante que la sécurité aux frontières d'un État[53]. Il sied de toute évidence que l'accent soit mis sur l'étude de cette convention, rappelons-le, seul texte international formel existant dans le domaine. Par ailleurs, en prenant le soin d'étudier l'ensemble des dispositions relatives à la cybersécurité adoptées au plan national, on conviendrait mieux de l'utilité du texte conventionnel dans la perspective d'une lutte ou de la création d'un cadre global de cybersécurité pouvant renforcer celle en vigueur au plan local.

L'intérêt ici étant de trouver un cadre légal global capable d'englober le cyberterrorisme et le cyberespionnage étatique, il apparaît primordial de montrer l'ampleur des risques des

[52] Pour un aperçu de l'interdépendance qui peuvent lier des infrastructures critiques, il est instructif de lire l'information sur le site Rfi.fr, en ligne : http://www1.rfi.fr/actufr/articles/044/article_23429.asp (consulté le 6 Mai 2014). L'article porte sur la panne informatique qui a paralysé les villes de New-York et Toronto en 2003.

[53] William DE LAAT, « The new perimeter initiative: will security trump trade? Cyber security and infrastructure the beyond the border action plan: a tool for enhanced Canada-U.S. cooperation on critical infrastructure and cyber security--or more window dressing? », **(**Automne 2012**)** 37 *Can.-U.S. L.J.* 451 1, 1-2.

cybermenaces décrites sur les intérêts d'un État, en mettant l'accent sur la vitalité des infrastructures essentielles par une analyse de leur rôle dans le fonctionnement de la société. L'évaluation ainsi faite des risques qui menacent de fragiliser l'État et la communauté internationale servira à cerner les défis qui leur sont posés. L'identification de ces risques permettra de mieux comprendre la réglementation de l'autorité canadienne. En outre, nous sommes d'avis que l'étude des dispositions conventionnelles à vocation pénale sera de nature à solutionner la question de l'imputabilité et de la qualification pénale des cybercrimes et apportera des indications des grandes lignes de défense numérique passive et active[54] nécessaires que devraient contenir les textes nationaux.

Il sied, pour cet argumentaire de définir dans un premier chapitre, la nature des MSP et des acteurs impliqués dans ces activités. Cela nous permettra de mieux comprendre le choix des dispositions nationales et régionales que nous étudierons dans le premier titre de ce mémoire. L'étude des institutions et des dispositions adoptées au plan national et la signature des ententes au plan régional nous permettra de définir l'étendue des dispositions déjà en vigueur sur le territoire. L'analyse de cette étude fournira des éléments d'appréciation des mesures adoptées par rapport aux risques que représentent les MSP. Ces insuffisances qui ressortiront de la première partie nous permettront de démontrer la considération des dispositions internationales existantes dans la lutte contre les MSP dans une perspective de garantie d'une paix et d'une stabilité numérique pérennes.

[54] S. GOODMAN, préc., note 34, p. 66.

TITRE 1 : La portée des MSP et la défense nationale actuelle

Le cyberterrorisme et le cyberespionnage étatique sont des dangers qui menacent la paix et la stabilité nationale. Elles exigent la mise en place de mesures de protection et de défense adéquates. Bien que l'on ne puisse rationnellement atteindre la disparition de ces menaces, force est de constater, suivant de nombreux experts, qu'il est possible de diminuer les vulnérabilités qui peuvent être exploitées. Puisque la cybersécurité ne se limite pas à un milieu géographique, elle nécessite une mobilisation internationale. Avant de procéder à l'étude des solutions que nous propose l'espace international actuel, nous analyserons dans ce premier titre, la portée des MSP (Chapitre 1) qui nous permettra de comprendre les mesures adoptées au plan national (Chapitre 2).

Chapitre 1 : La portée des MSP

Selon le ministre en charge du Ministère de la Sécurité publique du Canada (ci-après SP), les cybercrimes de type 1 représentent un danger pour la sécurité du Canada[55]. Il affirme :

> « Ils [Les services militaires et du renseignement étrangers, les réseaux criminels et les terroristes] s'emparent de nos systèmes informatiques, fouillent dans nos dossiers et provoquent des pannes informatiques. Ils volent nos secrets de sécurité nationale et industriels […]. »[56]

Ainsi résumé, les effets des MSP permettent de constater l'ampleur de ces activités en donnant un aperçu sur les « nouvelles armes » criminelles qui sont utilisées. Nous commencerons donc par entrer dans les méandres du cyberterrorisme (Section 1) pour ensuite aborder la notion du cyberespionnage étatique (Section 2). Enfin, nous appliquerons ces définitions aux cas recensés au cours des années. Cela nous permettra,

[55] Stratégie canadienne, préc., note 1, p.19-24 ; Il ne sera donc pas question dans notre étude, de nous prononcer sur les cybermenaces ou les cybercrimes ayant pour simple but, la poursuite de profits financiers.

[56] *Id.*, p. 3.

entre autres, de noter la sensible évolution qui va du profil-type de terroriste[57] et à celui de cyberterroriste. Nous remarquerons aussi que les États peuvent, du fait de leurs organes ou non, commettre des actes qui peuvent s'assimiler à du cyberterrorisme.

Section 1 : Les méandres du cyberterrorisme

Le cyberterrorisme est une notion qui tire sa source du terrorisme classique[58]. De fait, sur la scène internationale, il y a plusieurs catégories d'actes considérés comme relevant exclusivement du terrorisme classique [59] , mais qui sont plus caractéristiques de manifestations cyberterroristes. Étant une extension du terrorisme classique, le cyberterrorisme partage donc la même origine historique[60] et le même but, à savoir la

[57] Le profil-type du terroriste varie d'un auteur à autre. Ainsi, à l'époque moderne, pour Mario Bettati, le terroriste correspond aux extrémistes religieux en général, déduction qu'il tire de l'étude des stéréotypes décrits dans les bases de l'Interpol. Benoît Gagnon, ne se détourne pas de cette appréciation mais précise qu'il s'agit là des « nouveaux terroristes ». Les terroristes classiques étant reconnaissables à leurs revendications politiques alors que les nouveaux terroristes défendent des « discours nihilistes ». Il cite à cet effet Cindy C. Combs qui affirme que le niveau d'éducation et l'instabilité mentale fondent la naissance de ce type d'acteurs. Mario BETTATI, *Le Terrorisme les voies de la coopération internationale*, 1ère éd., Paris, Odile Jacob, 2013, p. 11-13; Charles Philippe DAVID et Benoît GAGNON (dir.), *Repenser le terrorisme Concepts, acteurs et réponses*, Québec, Les Presses de l'Université Laval, 2007, p. 56-58.

[58] Le terrorisme international classique est celui dont nous connaissons les manifestations depuis le Moyen-âge et dont le but est essentiellement la destruction physique de biens et actifs appartenant à un État. L'office de la langue Française le définit comme l'« ensemble des actes commis contre des biens ou des personnes, le plus souvent des civils, par une organisation qui se réclame d'une cause (politique, religieuse, etc.), dans le but de semer la terreur par la violence ou l'intimidation » pour préciser ensuite que « le terrorisme est notamment utilisé pour contraindre un gouvernement à agir, ou à s'abstenir d'intervenir, dans un contexte déterminé » OFFICE DE LA LANGUE FRANCAISE, « Le grand dictionnaire terminologique », (2002), disponible en ligne http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8354359 (consulté le 3 Septembre 2014).

[59] Des critères bien distincts permettent de catégoriser le cyberterrorisme. Il n'existe pas encore de cas officiellement enregistrés au niveau des instances internationales et de textes criminels le qualifiant expressément. Aviv COHEN, « Are we legally ready », **(**2010**)** 9 *J. Int'l Bus.& L.*1, 6-10. Au niveau de la classe doctrinale non plus, la distinction ne s'opère pas. C'est ainsi que Mario Bettati établi un large éventail des actes considérés comme étant une manifestation terroriste sans émettre une distinction entre eux. M. BETTATI, préc., note 57, p. 13; une autre confusion par rapport au « néologisme » survient aussi avec l' « hacktivisme politique ». La notion sera abordée *infra*, p. 23-24 ; Voir aussi G. KERSCHICHNIG, préc., note 33, p. 27-37.

[60] Tandis que certains auteurs associent la naissance du terrorisme avec l'avènement de la Révolution Française, d'autres par contre, identifient le début du terrorisme à la secte des Hashashims qui sévissait alors au Moyen-âge. Voir Pierre KLEIN, « Le droit international à l'épreuve du terrorisme », **(**2006**)** 321 *Recueil*

création, la propagation et l'entretien d'un climat de terreur[61]. Ces deux notions partagent *de facto* des critères communs, soit : (1) l'empreinte de la violence, (2) la défense d'une idéologie politique ou d'un idéal social ou religieux ainsi que (3) la volonté de semer la crainte au sein de la population. Cependant, comme le cyberterrorisme n'est qu'une branche du terrorisme classique, ces critères peuvent être présents à des degrés variés[62]. En outre, c'est l'environnement de commission qu'est le cyberespace[63] qui forme la particularité du cyberterrorisme. Cette particularité a également une incidence sur le type d'acteurs qui interviennent dans ces activités[64].

Ces indices qui permettent de reconnaître globalement un acte cyberterroriste ne comblent pas cependant l'absence de consensus international sur la définition du cyberterrorisme (Paragraphe 1). Par ailleurs, au-delà de l'éclaircissement terminologique qui ne fait qu'indiquer la reconnaissance de l'existence de la notion de cyberterrorisme par la communauté des États, l'ampleur factuelle du phénomène reste elle-même à préciser. Il faut donc considérer les capacités que le cyberespace offre aux cyberterroristes pour se rendre compte de l'ampleur de cette menace (Paragraphe 2).

Paragraphe 1 : Les définitions du cyberterrorisme

Comme mentionné plus haut, le cyberterrorisme découle du terrorisme et comporte la spécificité de son lieu de commission, le cyberespace. Confronté au risque élevé qu'il représente, plusieurs organisations internationales et autorités étatiques ont affirmé qu'il

---

des cours 203, 228. L'auteur rappelle l'origine du mot qui remonte à la période dite de Terreur qui a suivie la Révolution Française; voir aussi Marjie T. BRITZ, « The internet as a tool for terrorists: implications for physical and virtual worlds », dans Thomas J. HOLT, *Crime-on-line correlates, causes, and context*, 2nde ed., North Carolina, Carolina Academic Press, 2013, p. 161 ; M. BETTATI, préc., note 57, p. 42.

[61]P. KLEIN, préc., note 60; M. BRITZ, préc., note 60 ; Benoît GAGNON, préc., note 57, p. 56-58.

[62]Voir *infra*, p. 21-25.

[63] L'internet, utilisé en tant qu'outil ou cible fait partie des aspects qui entreront en compte dans la qualification d'un acte cyberterroriste dans notre étude. Des explications plus approfondies sont élaborées *infra*, p. 31-36.

[64]M. BETTATI, préc., note 57, p. 43. L'auteur effectue une analyse de la qualité des auteurs en suivant la nomenclature des années 2000 dressée par l'Union Européenne et le Département d'Etat américain.

incarne un danger pour la pérennité des nations[65]. De ces déclarations, il ressort une hétérogénéité de la conception du mot. Ces déclarations tracent néanmoins un éventail définitionnel (A) permettant de faire ressortir les critères de reconnaissance d'un acte cyberterroriste (B).

A. L'éventail définitionnel du cyberterrorisme

Barry C. Collins, précurseur du néologisme exposa pour la première fois les nouvelles ouvertures dont les terroristes bénéficiaient grâce aux nouvelles technologies[66]. Il affirmait d'ailleurs que l'intention des cyberterroristes était d'atteindre les mêmes fins que les terroristes classiques sans avoir à se salir les mains[67]. Dans le même ordre d'idée, le Conseil de l'Europe dresse un rapport dans lequel les risques du cyberterrorisme sont largement évalués. Le cyberterrorisme est ainsi défini très généralement comme l'utilisation de l'internet en tant qu'outil et cible dans la commission d'actes terroristes[68].

Il n'existe pas de texte international officiel qui énonce une définition du cyberterrorisme[69] ou qui y consacre des dispositions permettant de comprendre la signification même du concept[70]. A défaut, il est instructif de considérer ce que les

[65] Ce sont par exemple le Conseil de l'Europe et le Président des Etats-Unis. Voir par exemple Cyberterrorism, préc., note 18, p. 14 ; Barack OBAMA, « Taking the Cyberattack Threat Seriously », 19 Juillet 2012, The Wall Street Journal, disponible en ligne: http://www.wsj.com/video/taking-the-cyberattack-threat-seriously/ED29A414-7BAA-423F-8F9B-9AD49930F8F3.html?KEYWORDS=cyberattack+Obama (consulté le 6 Septembre 2014)

[66] Barry C. COLLIN, « The Future of Cyber Terrorism: Where the Physical and virtual worlds converge», **(**Mars 1997**)** 13 *Crime and Justice International* 2, disponible en ligne : http://www.cjcenter.org/cjcenter/publications/cji/ (consulté le 10 Avril 2014).

[67] M. IQBAL, préc., note 21, p. 403.

[68] Cyberterrorism, préc., note 18, p. 14.

[69] A. COHEN, préc., note 59; B. FOLTZ, « Cyberterrorism, computer crime, and reality», **(**2004**)** 12 *Information Management and computer security* 154-166.

[70] Il est cependant possible de déduire, de la qualification de certains actes, une catégorisation criminelle du cyberterrorisme, Cyberterrorism, préc., note 18, p. 52-97.

autorités des pays les plus industrialisés, considérés comme étant les plus interconnectés[71], en disent. En général, c'est la définition légale qui servira à qualifier le cyberterrorisme. Ainsi, au Canada, en regard à l'article 83.1 alinéa (b) du *Code criminel*[72], le SP expose que le cyberterrorisme est un ensemble de « *cyberopérations*» terroristes qui vise l'ébranlement du système étatique[73].

---

[71]Les pays industrialisés sont les plus touchés en raison de la forte connexion qui imprègne leur mode de vie. G. KERSCHISCHNIG, préc., note 33, p. 5.

[72] L'article énonce que le terrorisme est un acte d'omission ou de commission motivé par un idéal social religieux ou politique effectué dans l'optique de contraindre une population, un gouvernement ou une organisation internationale, pouvant causer de sérieux préjudices physiques, moraux, matériels, financiers capables de paralyser « des services, installations ou systèmes essentiels publics ou privés ». L'article 83 (1) b dispose ceci : « Soit un acte — action ou omission, commise au Canada ou à l'étranger :
(i) d'une part, commis à la fois :

- (A) au nom — exclusivement ou non — d'un but, d'un objectif ou d'une cause de nature politique, religieuse ou idéologique,
- (B) en vue — exclusivement ou non — d'intimider tout ou partie de la population quant à sa sécurité, entre autres sur le plan économique, ou de contraindre une personne, un gouvernement ou une organisation nationale ou internationale à accomplir un acte ou à s'en abstenir, que la personne, la population, le gouvernement ou l'organisation soit ou non au Canada,

(ii) d'autre part, qui intentionnellement, selon le cas :

- (A) cause des blessures graves à une personne ou la mort de celle-ci, par l'usage de la violence,
- (B) met en danger la vie d'une personne,
- (C) compromet gravement la santé ou la sécurité de tout ou partie de la population,
- (D) cause des dommages matériels considérables, que les biens visés soient publics ou privés, dans des circonstances telles qu'il est probable que l'une des situations mentionnées aux divisions (A) à (C) en résultera,
- (E) perturbe gravement ou paralyse des services, installations ou systèmes essentiels, publics ou privés, sauf dans le cadre de revendications, de protestations ou de manifestations d'un désaccord ou d'un arrêt de travail qui n'ont pas pour but de provoquer l'une des situations mentionnées aux divisions (A) à (C) ».

En se basant sur cette définition, le SP établit la similarité entre le terrorisme classique et le cyberterrorisme, le mode de commission introduisant une subtilité dans les deux terminologies. En ce sens, un acte de cyberterrorisme sera, par exemple, une cyberopération menée à des fins idéologiques dans le but de contraindre un gouvernement à accomplir un acte et qui sera de nature à compromettre sérieusement la sécurité d'une ou partie de la population.

[73] Stratégie canadienne, préc., note 1, p. 5. Par ailleurs, le gouvernement dresse une liste complète des groupes extrémistes qui menacent le gouvernement. Il est possible de la consulter en ligne : http ://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/index-fra.aspx (consulté le 12 Avril 2014). Ce type de terroristes n'est pas à confondre avec les cyberterroristes dont il n'existe pas encore de répertoire officiel au niveau national ou international. Il ne faut pas non plus confondre les cyberterroristes et les *hacktivistes politiques* comme les Anonymous. Ces derniers sont une autre typologie d'acteurs qui ne feront cependant pas l'objet d'une étude approfondie dans le cadre du présent travail. Pour en connaître, il est instructif de voir ce reportage de France 24 dans lequel un membre du réseau d'hackers Anonymous parle sous le micro France 24, disponible en ligne « Hackers, les nouveaux héros d'Hollywood », http ://www.france24.com/fr/20140314-gregg-housh-anonymous-houseofcards-netflix-hollywood-hackers-web-bernerslee-snowden-constitution-spritz/ (consulté le 15 Mars 2014).

Barack Obama a décrit en 2012 la dangerosité des cyberattaques, même s'il n'a pas émis de définition claire de l'acte cyberterroriste en lui-même[74]. Il a précisé globalement qu'il s'agissait d'activités susceptibles de causer un dommage à un pays par l'infestation ou la destruction d'une infrastructure critique.

Par ailleurs, plusieurs chercheurs, dont Dorothy Denning, ont consacré leurs études à la définition du cyberterrorisme. Selon cette dernière :

> « Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorisme, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. […] Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. »[75] [Nous soulignons]

L'auteure met l'accent sur la menace de l'activité sur les infrastructures essentielles d'un pays et du résultat destructeur majeur qui pourrait en résulter en raison de la forme de violence qui le caractérise. À la différence des autorités étatiques, elle précise la teneur de l'activité et met l'emphase sur la présence d'actes de violence, directs ou indirects, destinés à semer la terreur. En ce sens, Kelly Gable précise que le dessein de cette violence est d'exercer une contrainte sur les gouvernements :

> « criminal act conducted with computers and resulting in violence destruction, or death of its targets in an effort to produce terror with the purpose of coercing a government to alter its policies, and it includes attacks on computer networks and transmission lines within that definition»[76].

---

[74] B. OBAMA, préc., note 65

[75] Dorothy DENNING, *Cyberterrorism*, 1st ed., USA, Nova Science Publishers Inc, 2007, p. 71. Voir aussi Imran AWAN, « Cyber threats and cyber terrorism : The internet as a tool for extremism » dans Imran AWAN et Brian BLACKEMORE (ed.), *Policing cyber hate, cyber threats and cyber terrorism*, UK, Ashgate publishing, 2012, p. 23.

[76] K. GABLE, préc., note 23, p. 63.

En définitive, le cyberterrorisme semble être un acte pénalement répressible dont l'entendement général ne se dissocie pas du terrorisme classique[77]. Cette absence de définition commune est en partie justifiée par l'inexistence officielle d'acte de cyberterrorisme puisque « selon la majorité des spécialistes […], le cyberterrorisme fait partie des menaces en émergence »[78]. En effet, comme le soulignait Philip Brunst, aucun cas de cyberterrorisme officiel n'a encore été révélé probablement pour des raisons de secret gouvernemental[79]. Cependant, aujourd'hui, les avancées théoriques et la recherche de précision terminologique peuvent aller au-delà de la simple considération des capacités technologiques dont disposent les cyberterroristes[80]. Le piratage par des cyberterroristes du compte de l'État Islamique de la chaîne TV5, ou encore, celui du site de l'Association Internationale et Interdisciplinaire de la Chaîne de Médicaments (ci-après AIICM) en janvier 2015 viennent changer la donne[81]. Voir ci-dessous la capture d'écran du site piraté de l'AIICM :

[77] Jeffrey Thomas BILLER, *Cyber-Terrorism: Finding a Common Starting Point*, Thesis, Washington, Faculty of the George Washington University Law School, 2012, p. 24.

[78] C. P. DAVID et B. GAGNON, préc., note 57, p. 258; Cyberterrorism préc., note 18, p. 16.

[79] Selon Phillip Brunst, certaines cyberattaques terroristes ont déjà été répertoriées mais ont été gardées sous le sceau du secret gouvernemental. Il affirme: « according to the informal sources, cyberterrorist attack have already taken place and are posing an actual threat to the security of important infrastructures. However, most cases are kept confidential to protect the safety of affected state and other similarity affected infrastructures. Accordingly, current literature often only contains potential or realistic scenarios. Whether these settings have actually taken place, however, is rarely known ». Cyberterrorism, préc., note 18, p. 16 [note 9]. Voir aussi: Christopher E. LENTZ, « A State's Duty to Prevent and Respond to Cyberterrorist Acts », **(**2009-2010**)** 10 *Chi. J. Int'l L.* 799, 799-820; Tara Mythri RAGHAVAN, « In fear of cyberterrorism: an analysis of the Congressional response», **(**2003**)** *U. Ill. J.L. Tech. & Pol'y* 297, 297.

[80] Il est intéressant de porter un regard sur la théorie du *Keep It Simple Stupid* (KISS) qui avance que dans une société, tous les individus aient accès aux mêmes outils dans leur quotidien. Les terroristes ont donc accès aux mêmes outils et peuvent donc en faire usage. C.P. DAVID et B. GAGNON, préc., note 57, p. 244.

[81] Voir note 24, pour plus d'informations. Cette attaque a fait réagir les autorités françaises, notamment Bernard Cazeneuve qui, cité par le Libre.be, affirme : « "Nous avons décidé d'armer davantage nos services pour faire face et prévenir ce type d'attaques (...) ce qui vient de se passer témoigne de la pertinence des actions que nous avons engagées", a-t-il dit, au sujet notamment du projet de loi sur le renseignement en cours d'examen au Parlement » ; Libre.be, « Piratage de TV5Monde : le gouvernement français "déterminé" à combattre "des terroristes" » **(**9 Avril 2015**)**, disponible en ligne http://www.lalibre.be/actu/international/piratage-de-tv5monde-le-gouvernement-francais-determine-a-combattre-des-terroristes-55263da835704bb01ba8830f (consulté le 9 Avril 2015); aussi disponible en vidéo : http://www.lemonde.fr/pixels/video/2015/04/09/tv5-les-pirates-seront-mis-hors-d-etat-de-nuire_4612481_4408996.html (consulté le 9 Avril 2015).

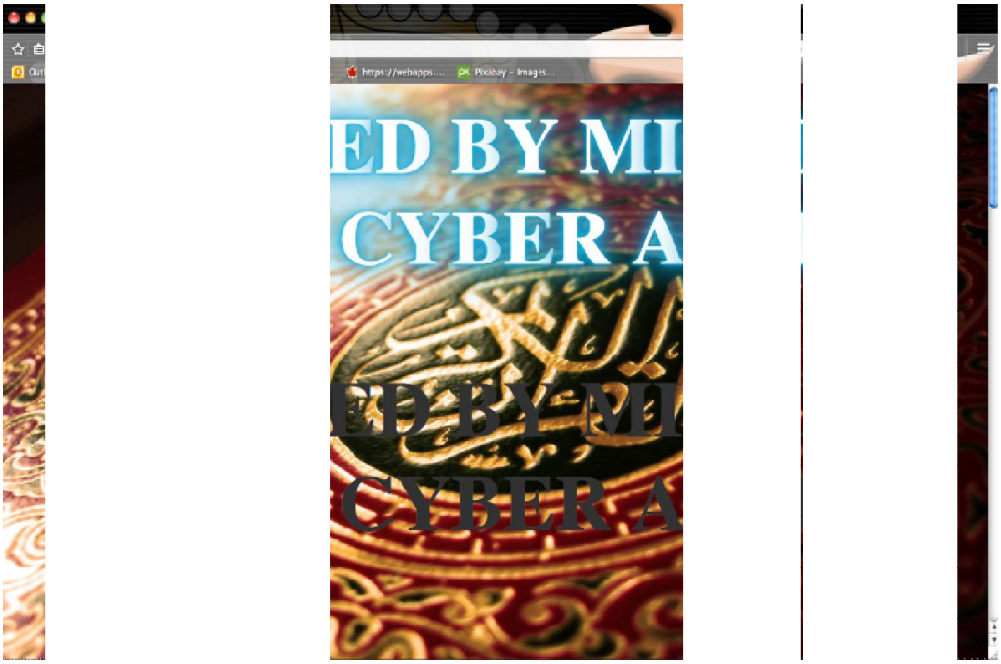

Figure 1 : Image d'un site piraté

Pour l'élaboration de ce travail, le cyberterrorisme sera défini au regard des différentes composantes recensées à partir des définitions susmentionnées. Il pourrait alors s'entendre d'une activité ou d'un ensemble d'activités informatiques destinées à porter atteinte aux infrastructures importantes d'un pays afin de causer de sérieux dommages à une Nation et à son gouvernement. Cette définition large ne permettant pas de cerner complètement la notion, il importe de porter un regard sur les buts de l'activité que sont la propagande, le recrutement, la recherche de financement et la désinformation[82]. Ces objectifs sont similaires à ceux du terrorisme, mais leur atteinte appelle une manœuvre plus simple exacerbant l'incidence de leurs actions auprès de la classe civile, plus à risque[83]. De plus, la technologie amène à une révision de la notion de violence. L'activité doit être à présent considérée dans une dimension plus large[84]. En l'absence de définition officielle, il est

[82] M. BRITZ, préc., note 60, p. 166.

[83] C'est d'ailleurs en cela que Barry Collins affirmait la facilité qui caractérisait les actes des cyberterroristes. Voir B. C. COLLINS, préc., note 66.

[84] Clay WILSON affirme que la difficulté de la définition du cyber terrorisme réside dans l'imprécision des auteurs de l'acte, des motivations et des intentions de ceux-ci. Clay WILSON, « Botnets, Cybercrime, and

possible de se baser sur les différentes composantes de l'acte pour comprendre le concept de cyberterrorisme.

B. Les critères de reconnaissance d'un acte cyberterroriste

Afin d'aboutir à une précision des critères de reconnaissance d'un acte cyberterroriste[85], il faut considérer 1) la typologie des acteurs, 2) leurs motivations et 3) les cibles visées. Tel qu'annoncé plus haut, en raison de l'inexistence d'instruments internationaux communs et de textes nationaux pertinents, la précision des éléments de l'acte sera déduite des composantes du terrorisme classique.

Ainsi, lorsqu'on se rapporte à la typologie d'un terroriste, telle qu'il ressort des standards dressés par le Département d'État américain[86], le Conseil de l'Europe[87] et le SP[88], on constate que l'emphase est mise sur son origine sociale, à son âge[89] et à son sexe[90].

D'un milieu à l'autre, la méthode de recrutement diffère. Ainsi, dans un milieu islamisé, ce seront les jeunes religieux pratiquant qui seront recherchés et qui agiront dans le but

---

Cyberterrorism: Vulnerabilities and Policy Issues », **(**2008**)** *Cong. Research Serv* cité par J. T. BILLER préc., note 77, p. 24.

[85]Une conception claire de l'acte cyberterroriste permet de définir les contours d'un texte légal spécifique et d'entreprendre la mise en œuvre de mesures de répression efficaces. Voir : A. COHEN, préc., note 59, p. 7.

[86] U.S. DEPARTMENT OF STATE, *Foreign Terrorist Organizations*, 28 Septembre 2012, en ligne http://www.state.gov/j/ct/rls/other/des/123085.htm (consulté le 3 Avril 2014).

[87]M. BETTATI, préc., note 57, p. 44.

[88] MINISTERE DE LA SECURITE PUBLIQUE DU CANADA, *Liste des entités terroristes inscrites*, en ligne http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-fra.aspx (consulté le 3 Avril 2014).

[89] Le professeur Mario Bettati établit une générale classification sociale du terroriste des années 2000 en se basant sur les répertoires des organes internationaux de renseignements, notamment Interpol. Pour plus d'informations, voir M. BETTATI, préc., note 57, p. 44.

[90]*Id*., les potentiels terroristes sont donc des hommes et, dans de rares exceptions, des femmes (qui agissent de façon plus sournoise puisqu'elles sont moins considérées à risque). France24.com, « Enquête : pourquoi il ne faut pas sous-estimer le rôle des femmes jihadistes » **(**14 Février 2014**)**, disponible en ligne http://www.france24.com/fr/20150204-organisation-etat-islamique-femmes-jihadistes-mariage-combattante-facebook/ (consulté le 14 Février 2014).

« d'assainir les occidentaux du péché » tandis que, dans un milieu occidental, le recrutement se basera sur l'appartenance culturelle et la précarité du milieu de vie[91]. Mario Bettati explique que ce sont souvent des générations d'immigrants qui entretiennent une haine contre leur pays d'accueil[92].

Un autre portrait-type de terroriste porte sur les individus n'ayant aucun antécédent judiciaire[93] et libres de sérieuses attaches religieuses[94]. Ils peuvent être contactés de différentes façons par les groupes terroristes qui les plongent dans leur propagande d'endoctrinement. Ce recrutement est davantage orienté vers des jeunes psychologiquement faibles[95]. C'est d'ailleurs cette dernière génération de potentiels terroristes qui correspond davantage au profil des cyberterroristes actuels[96].

Dans une relation de cause à effet, ce seront ces jeunes qui chercheront le plus à socialiser sur les réseaux sociaux pour s'y créer un monde où ils gèrent leurs relations interpersonnelles, subissant ainsi l'influence des médias et de groupes extrémistes

---

[91] *Id*.; G. WEIMANN, *www.terror.net. How Modern Terrorism Uses the Internet*, préc., note 22, p. 8-9.

[92] M. BETTATI, préc., note 57, p. 45.

[93] Paul WILKINSON, « Enhancing Global Aviation Security », dans Paul WILKINSON et Brian M. JENKINS (ed.), *Aviation terrorism and security*, Portland, Frank Cass, 1999, p. 51.

[94] Dounia BOUZAR, Christophe CAUPENNE et Sulayman VALSAN, « La métamorphose opérée chez le jeune par les nouveaux discours terroristes. Recherche-action sur la mutation du processus d'endoctrinement et d'embrigadement dans l'islam radical », Novembre 2014, disponible en ligne http://www.bouzar-expertises.fr/metamorphose (consulté le 18 Novembre 2014).

[95] *Id*.; Djemila BENHABIB, « Carton rouge pour les djihadistes canadiens : bye bye le passeport », **(**24 Septembre 2014**)**, disponible en ligne http://actualites.sympatico.ca/nouvelles/blogue/carton-rouge-pour-les-djihadistes-canadiens-bye-bye-le-passeport (consulté le 18 Novembre 2014); Eugénie BASTIÉ, « Le profil inattendu des djihadistes français », **(**18 Novembre 2014**)**, en ligne www.lefigaro.fr/actualite-france/2014/11/18/01016-20141118ARTFIG00158-le-profil-inattendu-des-djihadistes-francais.php (consulté le 18 Novembre 2014); D. BOUZAR, C. CAUPENNE et al, préc., note 92; C. P. DAVID et B. GAGNON, préc., note 57, p. 58.

[96] Phillip Brunst explique que l'utilisation de l'internet par les terroristes leur permet de recruter à travers le monde de nouveaux types de terroristes. En témoigne les récents enrôlements de jeunes, a priori non à risque, dans le djihad. Cyberterrorism, préc., note 18, p. 37; Sur le même ton, Cindy Combs mentionne : « […] althought the majority of active terrorists are in their twenties, there has been a tendency, particularly among the Arab and Iranian groups, to recruit children of 14 or 15 years of age ». L'auteur est citée dans C.P. DAVID et B. GAGNON préc., note 57, p. 67.

activement présents sur ces réseaux[97]. C'est par ce canal que les groupes terroristes procèdent à leur prosélytisme. Dans ce processus, le statut social de l'individu ne permet pas systématiquement de le catégoriser puisqu'il a peu d'importance sur le réseau social[98]. Il n'existe pas non plus de frontière géographique propice à un embrigadement basé sur la crainte des traditions[99].

Grâce aux moyens d'action contemporains et diversifiés dont il dispose, le cyberterroriste utilise l'internet comme outil et/ou cible[100].

Les motivations d'une cyberattaque terroriste[101] visent l'effondrement d'une puissance étatique[102] en faisant usage de violence[103] avec l'intention de semer de la peur. Ces

[97] Reportage FrTv, « Affaire MERAH, Itinéraire d'un tueur », disponible en ligne https://www.youtube.com/watch?v=Q3GS0d0N390 (consulté le 17 Octobre 2014). Dans ce dossier, il est intéressant d'apprendre comment le jeune djihadiste, qui s'est servi de l'internet pour rechercher des bases d'entraînements au Pakistan. Il s'en est également servi pour regarder les vidéos de propagande qui ont alimenté son intention d'agir à l'encontre des Etats occidentaux, en l'occurrence la France et le Canada (mention en faite après la première heure du documentaire). Le documentaire montre aussi la disponibilité sur internet de directives pour apprenti djihadiste (à 1h30). Il est également possible de trouver en ligne des outils d'informations sur les cibles à attaquer, un historique des scores des attaques que d'autres djihadistes ont mené ou encore les cibles vulnérables dans le pays. Voir Larry GREENEMEIER, « Electronic Jihad' App Offers Cyberterrorism For The Masses », **(**7 Juillet 2007**)**, disponible en ligne : http://www.informationweek.com/electronic-jihad-app-offers-cyberterrorism-for-the-masses/d/d-id/1056683 (consulté le 17 Août 2014); Caroline POLITI, « le Normand devenu égorgeur pour Daech », **(**17 Novembre 2014**)**, disponible en ligne : http://www.lexpress.fr/actualite/societe/maxime-hauchard-le-normand-devenu-egorgeur-pour-daesh_1622739.html#IJpLyH0JuM2cf51d.99 (consulté le 17 Novembre 2014); Lefigaro.fr, « Un Normand de 22 ans figure parmi les bourreaux de l'État islamique », **(**17 Novembre 2014**)**, disponible en ligne : www.lefigaro.fr/actualite-france/2014/11/17/01016-20141117ARTFIG00081-un-normand-de-22-ans-soupconne-d-etre-l-un-des-bourreaux-de-peter-kassig.php (consulté le 17 Novembre 2014).

[98] C'est le cas d'Umar Farouk Abdulmutallab, étudiant « modèle » de l'University College de Londres entre 2005 et 2008, issu de la bourgeoisie nigérianne qui essaya de faire exploser un vol en direction des Etats-Unis. Selon les dires de sa famille, il subissait une grande influence sur l'internet. Pour plus d'informations, Johan HUFNAGEL, « Umar Farouk Abdulmutallab: questions pour un attentat raté » 27 Décembre 2009, disponible en ligne : www.slate.fr/story/14983/umar-farouk-abdulmutallab-une-faq-attentat-detroit-amsterdam-al-qaida (consulté le 5 Avril 2014).

[99] M. BETTATI, préc., note 57, p. 45.

[100] En ce sens, l'internet est utilisé comme outil lorsque, par exemple, un cyberterroriste qui utilise la connexion pour déclencher l'activation d'une bombe ne brise pas la connexion mais l'utilise pour atteindre sa finalité. L'internet ou la technologie est utilisé comme cible lorsque la finalité de l'attaque est de porter atteinte directement au réseau. Cette offensive doit cependant aboutir en utilisant le réseau lui-même ou une technologie quelconque pour le détruire. Cyberterrorism, préc., note 18, p. 26.

[101] Les cyberterroristes peuvent aussi cibler le réseau. Dans cette logique, il est possible de présumer qu'ils viseraient donc sa destruction complète. Cela reste peu probable au su de l'importance que cet outil revêt

terroristes engagent des combats « sans revendication claire et basé sur des idéologies millénaristes ou extrémistes »[104].

En outre, la cible d'une attaque cyberterroriste est difficilement discernable tant que les dégâts ne sont pas encore causés. Aussi, ce n'est que lorsque le mal est fait qu'il est possible de comprendre l'intention finale des auteurs. *A pari*, on peut déduire que les motivations des cyberterroristes découlent de leur source, le terrorisme classique. De même, le cyberterrorisme viserait la déstabilisation ou l'affaiblissement d'un État[105].

Mentionnons au passage que ce type de cyberterroriste pourrait s'assimiler aux *hacktivistes*. Il s'en distingue pourtant. Le combat de ces *hacktivistes* est généralement orienté contre certaines politiques gouvernementales qu'ils jugent incorrectes, comme le font les *Anonymous*, par exemple, qui s'autoproclament les *gardiens du web* et pratiquant de l'*hacktivisme malveillant*[106]. La différence majeure qui existe entre ces hackers et les

---

pour leurs organisations. Ceci est tout de même paradoxal puisqu'il ne correspond pas réellement à la finalité suprême qu'ils revendiquent, à savoir la fin du monde occidental. Car, en effet, si cela était, l'internet serait leur première cible, étant un pur produit des américains, cible par excellence de ses cybercriminels.

[102]Cyberterrorism, préc., note 18, p. 34-38. L'effondrement de la puissance étatique passe par l'atteinte de deux objectifs à savoir la confusion économique (« economic confusion ») et la discrimination de l'opposant (« opponent discrimination »). La déstabilisation d'un État vise alors à prouver au monde la vulnérabilité de ses infrastructures de défense et la manque de compétences techniques que cet État possède.

[103]L'intrusion illégale dans un réseau a pour objectif de causer un dysfonctionnement ou une rupture dans le système de façon à désorganiser l'ordre normal de fonctionnement de l'infrastructure visé. Cela a pour effet direct de créer une tension au niveau de la société, au niveau gouvernemental lui-même ou à l'échelle internationale lorsque l'agression cybernétique implique une multiplicité d'attaques. On peut alors considérer qu'il s'agit d'une violence indirecte.

[104] C.P. DAVID et B. GAGNON, préc., note 57, p. 57. A cet effet, les auteurs citent Matthew J. Morgans qui écrit : « where secular terrorists regard violence either as a way of investigating the correction of a flaw in a system, that is basically good or as a means to foment the creation of new system, religious terrorists see themselves mot as a components of a system worth preserving but as "outsiders", seeking fundamental changes in the existing order. This sense of alienation also enables the religious terrorist to contemplate far more destructive and deadly types of terrorist operations than secular terrorists, and indeed to embrace far more open-ended category of "enemies" for attack ». Matthew J. MORGANS, « the origins of the new terrorism », **(**Printemps 2004**)** 34 1 *Parameters*.

[105] La majeure partie des terroristes classiques et des cyberterroristes ont pour principal objectif l'effondrement de la puissance occidentale et américaine par une destruction de leurs organes administratifs essentiels. J. T. BILLER, préc., note 77, p. 25.

[106] Étude hors-série*,* préc., note 11, p.27.

cyberterroristes, tels qu'étudiés dans ce travail, repose sur l'absence de propagande des groupes de hackers qui ne font que de la protestation politique sans intention de créer une armée de défenseurs ou de s'entourer de personnes véhiculant leurs idéologies[107]. Phillip Brunst[108] affirme : « a [cyber]terrorist typically takes a long-terme perspective »[109]; cela reste toutefois sujet à débat[110].

Une autre distinction peut également être faite entre le cyberterrorisme et le *technoterrorisme*. Le cyberterrorisme passe par l'informatique et peut entraîner la destruction d'un bien physique alors que le technoterrorisme consiste à exercer une violence directe (cinétique) contre des installations informatiques[111].

A l'instar du cyberterroriste agissant pour son propre compte ou celle de son organisation, certains Etats sont également dénoncés comme menant des activités cyberterroristes, c'est-à-dire des assauts contre les systèmes numériques d'infrastructures critiques d'autres Etats. Le cyberterrorisme parrainé par des Etats implique des pirates informatiques (*hackers*) qui, apportent leur savoir-faire à la commission de l'acte. Ces États agissent

[107] Alexandra Whitney SAMUEL, *Hacktivism and the future of political participation*, Thesis, Cambridge, Harvard's university, 2005, disponible en ligne: http://search.proquest.com/docview/60705513?accountid=12543 (consulté le 4 Juillet 2014).

[108]Cyberterrorism, préc., note 18, p. 18.

[109] C. TOMUSCHAT, « On the possible « added value » of a comprehensive Convention on Terrorism », **(**2005**)** 26 *Human Rights Law Journal* 287, 287-306, cité par Cyberterrorism, préc., note 18.

[110] En effet, il est d'avis dans ce travail que même les hacktivistes malveillants planifient sur une certaine durée leurs cyberattaques en espérant marquer profondément les esprits et démontrer la faiblesse des protections numériques d'un État. Voir par exemple le documentaire Pièce à conviction, *Anonymous, la guerre est déclarée*, en ligne https://www.youtube.com/watch?v=mpHJwW258gs (consulté le 12 Octobre 2014).

[111] C.P. DAVID et B. GAGNON, préc., note 57, p. 260; L'auteur explique que le technoterrorisme serait donc une forme de terrorisme qui viserait les infrastructures d'informations de manière physique; il s'agirait par exemple, de détruire un système informatique avec une bombe. De son côté, le cyberterrorisme viserait à frapper les infrastructures de manière virtuelle à des fins de destruction, de contrôle ou de vol de données. »

alors par le biais d'intermédiaires pour commettre ce que le ministre du SP qualifie de « sabotage et d'ingérence étrangère »[112].

En considérant par exemple les cyberattaques qui impliquent des terroristes islamistes, il est possible de constater que les effets recherchés sont en général l'interruption ou la destruction de systèmes informatiques ou de biens physiques.

Paragraphe 2 : Les avantages qu'offre le cyberespace

Sans exposer de cas précis de cyberattaques terroristes menées par des acteurs islamistes, l'OCDE évoque que les conséquences d'une cyberattaque terroriste, telle que la destruction des actifs d'un État ou encore la propagande de terreur, constituent une menace et un danger avéré pour la population civile, la paix et la sécurité étatique[113]. Son incidence ne se limite pas à insuffler de la peur au sein d'une Nation ou encore à ébranler un État. Rappelons que la technologie et l'internet propulsent ses effets à l'échelle internationale, sans autrement inquiéter les terroristes à qui les structures interconnectées du cyberespace procurent une bonne couverture.

L'internet offre aux cyberterroristes les avantages d'une « guerre de salon »[114] Ces derniers peuvent utiliser l'internet comme outil, pour la communication ou pour la planification de leurs activités (A), ou comme cible, en visant la destruction d'un réseau (B).

[112] Stratégie canadienne, préc., note 1, p. 6; Paul N. STOCKTON et Michele GOLABEK-GOLDMAN, « Prosecuting cyberterrorists: applying traditional jurisdictional frameworks to a modern threat » **(**2014**)** 25 *Stan. L. & Pol'y Rev.* 211, 218.

[113]Conseil de l'OCDE, préc., note 39.

[114] Cette expression renvoie au cyberwarfare qui ne nécessite pas de déploiement sur un terrain de combat physique mais qui se déroule uniquement sur le web. B. GAGNON, préc., note 8.

A. L'internet utilisé comme outil

Pour les cyberterroristes, l'internet est comme une arme à feu qui ne s'enraye pas, toujours à portée de main et dont les munitions ne s'épuisent jamais. L'internet comme outil de recrutement[115] leur sert à mener à bien leurs activités de prosélytisme qui se déroulent la majeure partie du temps sur les réseaux sociaux par la diffusion de vidéos d'attentats, d'exécutions filmées et d'informations erronées[116]. L'internet est également un outil de communication[117] qui permet aux cyberterroristes d'échanger entre eux, en multipliant les encodages afin d'embrouiller les pistes d'enquêtes[118]. Comme mentionné plus haut, le réseau permet également aux cyberterroristes de faire du recrutement, de tenir des formations à l'endroit des nouveaux membres, d'obtenir du financement et d'effectuer des levées de fonds[119]. Outre la « sécurité et la pérennité » qu'il offre aux terroristes et qui leur permet de mener des actions furtives, ces actions ont des répercussions importantes sur les infrastructures physiques[120].

L'utilisation de matériel informatique et du réseau internet pour faire circuler de l'information et opérer leur recrutement est une étape centrale de l'élaboration d'un acte terroriste et existait déjà dans le terrorisme classique. Ce procédé définit toutefois les

[115]Le cyberterrorisme étant une activité cybercriminelle, il est intéressant de porter un regard sur l'utilisation de l'internet et de l'outil informatique dans la commission du cybercrime en général. Voir MINISTERE DE L'INDUSTRIE, *Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police*, Centre canadien de la statistique juridique, N° 85-558-XIF, Ottawa, 2002, p. 6 ; A. COHEN, préc., note 59, p. 6 ; Affaire Merah, préc., note 97.

[116]Gabriel WEIMANN, « Terror on the internet: the new arena, the new challenges» **(**2006**)** 4 10 *Middle East Journal* 60, 777-788, http://search.proquest.com/docview/36533923?accountid=12543(consulté le 19 Avril 2014); Cyberterrorism, préc., note 18, p. 15-47.

[117] I. AWAN et B. BLACKEMORE, préc., note 75, p. 27-32.

[118] G. WEIMANN, *www.terror.net. How Modern Terrorism Uses the Internet*, préc., note 22, p. 3; Cyberterrorism, préc., note 18, p. 15-47; Pour Daniel Fromson, l'internet aura énormément servi au groupe Al Quaïda dans l'attentat du 9/11. Ils l'auraient utilisé pour une planification précise de l'activité en raison des communications plus aisées. Voir : Daniel FROMSON, « Weapons of mass » **(**2010**)**, 09 *Harper's Magazine* 54, disponible en ligne http://search.proquest.com/docview/749163600?accountid=12543 (consulté le 13 Novembre 2014).

[119] G. WEIMANN, *www.terror.net. How Modern Terrorism Uses the Internet*, préc., note 22, p. 7.

[120] C.P. DAVID et B. GAGNON, préc., note 57, p. 264.

caractéristiques du cyberterrorisme[121] car il constitue l'indicateur des facilités à portée des acteurs[122].

B. L'internet utilisé comme cible

Nous soulignons tout d'abord que ce sont les interconnexions d'un réseau qui peuvent être prises pour cible par les cyberattaques terroristes, et non la structure internet en entier. En effet, même si sa destruction était envisageable, il est impensable que des organisations terroristes telles qu'Al Quaida par exemple veuillent ruiner un atout précieux de leur propagande.

Ainsi, en visant la structure numérique d'une infrastructure critique telle que celle des télécommunications canadiennes, les terroristes pourraient interrompre la communication entre les services d'urgence et les personnes en situation précaire ayant un besoin d'aide. Les contrevenants pourraient par exemple provoquer un bug informatique[123] dans un système aérien paralysant les vols de nombreuses compagnies et causant d'importants préjudices économiques. Les terroristes ont également la capacité d'interrompre des

[121] Malgré la tendance qui veut que l'utilisation de l'internet comme outil serait le fait de la totalité des organisations terroristes, il existe encore certaines d'entre elles qui se servent des moyens traditionnelles de recrutement comme la pêche de rue ou les interventions sur les places publiques destinés à tenir le monde au courant des abus du monde occidental et à rassembler une foule au sein de laquelle s'opère un recrutement massif. C'est le cas du groupuscule Sharia for Belgium actuellement poursuivi par le Ministère public belge : « Le méga-procès pour terrorisme de Sharia4Belgium se poursuit à Anvers », en ligne http://www.rtbf.be/info/belgique/detail_le-proces-pour-terrorisme-de-sharia-for-belgium-debute-a-anvers?id=8366206 (consulté le 12 Octobre 2014).

[122] Des cas mis en avant de l'utilisation de l'internet dans la commission des attaques cyberterroristes, il ressort que le réseau est beaucoup plus utilisé comme un outil plutôt que cible. En tant que cible, si le réseau était visé dans le but de le détruire totalement, il serait défavorable pour les cyberterroristes de perdre un outil aussi précieux et de détruire une bonne quantité de données par lesquelles ils mènent la quasi-totalité de leurs activités. Cyberterrorism, préc., note 18, p. 28 et 46.

[123]Il est intéressant de porter une attention sur les conséquences économiques du bug informatique qui a affecté le système aérien de Londres le 12 Décembre 2014. Voir en ligne : http://www.air-journal.fr/2014-12-13-bug-monstre-a-londres-encore-38-annulations-ce-samedi-5127972.html (consulté le 13 Décembre 2014).

systèmes d'alimentation énergétiques[124] comme la coupure d'électricité qui a affecté les États-Unis en 2003[125].

Afin de mener les cyberattaques, les cyberterroristes envoient très souvent des dénis de service[126] pour créer un dysfonctionnement des connexions du réseau comme ce fut le cas au Moyen-Orient où des pirates israéliens bloquèrent l'accès à de nombreux sites internet palestiniens[127]. Ce fut également le cas des attaques lancées contre les institutions des États-Unis et de la Corée du Sud[128]. Par ailleurs, les cyberterroristes peuvent aussi se servir d'outils conventionnels de *hacking*[129]. Ils peuvent aussi mener une attaque

[124]A. COHEN, préc., note 59, p. 3 et 5; S. GOODMAN, préc., note 34; Cyberterrorism, préc., note 18, p. 17-46.

[125] Un cas similaire de coupure d'électricité par-delà la frontière canado-américaine s'est déjà produite en 2003 et s'est étendue du Nord-Est des Etats-Unis à Toronto et a d'abord paru être l'œuvre de terroriste selon le président américain Georges W. Bush. Il s'agissait finalement d'une simple panne. Cette situation semble démontrer que ce genre d'hypothèse constitue déjà une situation de cyberattaque plausible que le gouvernement américain redoute. Voir note 52.

[126]Le DDoS est une technique d'attaque qui consiste à saturer un serveur « cible par un assaut répété et simultané qui l'oblige à arrêter de fournir du service ou qui vise à la ralentir. Pour plus d'informations sur le sujet, voir G. KERSCHICHNIG, préc., note 36, p. 34; J. A. CHANDLER, préc., note 26, p. 236-240. L'auteur rappelle, par exemple, le déni de service qui avait affecté le système d'enregistrement d'Air Canada. Elle écrit : « [A worm] known as 'Welchi', 'Welchia' […] which was actually intended to protect computers […] brought down the Air Canada chek-in system, infiltrated unclassified computers on the U.S. navy intranet […] », p. 237;voir aussi en ligne : « http://www.mcafee.com/us/downloads/free-tools/ddosping.aspx » (consulté le 10 Juin 2014); voir aussi : B. GAGNON, préc., note 8. Pour plus d'informations sur les manœuvres des cyberattaques, voir R. NGUYEN, préc., note 12, p. 1093-1098.

[127] En Septembre 2000, des pirates israéliens créèrent un incident international en bloquant l'accès à de nombreux sites internet palestiniens, faisant planer le risque d'une cyberguerre. Voir en ligne http://www.haaretz.com/weekend/magazine/israeli-hacker-turned-brain-researcher-making-waves-1.405844 (consulté le 13 Juin 2014).

[128] En Juillet 2009, certaines connexions d'organismes stratégiques de la Corée du Sud et des Etats-Unis ont été victimes de l'invasion d'un ver informatique dont la source précise n'a jamais pu être identifiée. Aux dires de l'Agence du renseignement sud-coréen, l'attaque provenait de 86 adresses IP situés dans 16 pays. Pour de l'information globale sur les différentes cyberattaques chinoises, voir généralement Bryan KREKEL, « Capability of the People's Republic of China to conduct cyberwarfare and computer network exploitation », **(**2009**)** *US-China Economic and Security Review Commission* dans BIBLIOTHÈQUE DU PARLEMENT, *Cybersécurité et renseignement de sécurité : l'approche des États-Unis*, n° 2010-02-F, Service d'information et de recherches parlementaires, 2010, p. 1 [note 2].

[129]Cyberterrorism, préc., note 18, p. 23-26.

informatique contre un réseau et lancer parallèlement, une attaque physique contre des infrastructures[130].

De même, lors de l'attaque cyberterroriste du 9 avril 2015 contre TV5, les acteurs ont exposé des messages de propagande menaçant l'État français, le président François Hollande[131], ainsi que les soldats du pays[132]. Le directeur de la chaîne, Yves Bigot, affirmait :

> « Nos systèmes ont été extrêmement détériorés par cette attaque d'une puissance inouïe et le retour à la normale va prendre des heures, voire des jours »[133].

Les attaques cyberterroristes menacent dangereusement la stabilité de l'État[134]. Ces menaces internationales sont exacerbées par les avancées technologiques[135]. Les groupes terroristes sont continuellement en attente de failles de sécurité pour lancer des attaques contre les infrastructures et les biens symbolisant la puissance d'un État[136]. Même si la préparation d'une attaque cyberterroriste peut faire appel à de grandes capacités humaine,

---

[130] *Id.,* p. 26-27.

[131] Francetvinfo.fr cite les messages publiés sur la page facebook de la chaîne TV5 : « Le message accusait le président français, François Hollande, d'avoir commis *"une faute impardonnable"* en menant *"une guerre qui ne sert à rien". "C'est pour ça que les Français ont reçu les cadeaux de janvier à Charlie Hebdo et à l'Hyper Cacher",* ajoutaient les pirates […] » . Voir sur FranceTvInfo.fr, « Ce que l'on sait du piratage de la chaîne TV5 Monde par des individus se réclamant du groupe Etat islamique », disponible en ligne : http://www.francetvinfo.fr/monde/proche-orient/offensive-jihadiste-en-irak/la-chaine-tv5-monde-victime-d-un-piratage-de-grande-ampleur-par-des-individus-se-reclamant-du-groupe-etat-islamique_871789.html (consulté le 9 Avril 2015).

[132] *Id*., Après avoir posté des détails confidentielles sur la page Facebook de soldats français en mission contre l'EI, ils affichèrent des messages de propagande qui se lisent comme suit : *«* Soldats de France, tenez-vous à l'écart de l'État islamique ! Vous avez la chance de sauver vos familles, profitez-en" "Au nom d'Allah le tout Clément, le très Miséricordieux, le Cyber Caliphate continue à mener son cyberjihad contre les ennemis de l'État islamique ».

[133] Voir note 24.

[134] Susan W. BRENNER et Marc D. GOODMAN, préc. note 19, p. 1-11. Dans cet article, les auteurs avancent plusieurs cas de cyberattaques terroristes qui pourraient ébranler l'intégrité étatique.

[135] Cyberterrorism, préc. note 18, p. 16; M. POLLIT, *Cyberterrorism –Fact or fancy ?*, 20th National Information Systems Security Conference, 1997, p. 285-289.

[136] R. RADVANOVSKY et A. MCDOUGALL, préc., note 38, p. 17-22.

technique et financière, le risque n'est pas écarté[137]. Il justifie la mise en place rapide et complète d'un cadre global de prévention et de riposte sûres.

Section 2 : Le cyberespionnage étatique

Au rang des cybercrimes de type 1, le cyberespionnage étatique appelle des manœuvres similaires[138] à celles du cyberterrorisme mais est mené à des fins stratégiques militaires. Si, le cyberterrorisme et le cyberespionnage d'origine étatique sont tous deux menées à l'aide d'outils informatiques similaires, ils n'ont pas les mêmes finalités. En effet, le cyberespionnage étatique est considéré comme une stratégie militaire mise en place par des gouvernements afin d'asseoir leur puissance[139]. L'exécution d'un cyberespionnage étatique se réalise sur une moyenne ou longue durée dépendamment des objectifs visés[140]. Selon son ampleur, il nécessite l'utilisation d'outils et de logiciels qui peuvent être complexes et dispendieux et qui ne sont généralement pas accessibles à des groupes idéologiques ou religieux épars[141].

[137] Cyberterrorism, préc., note 18, p. 44; Clay WILSON, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service Report (RL 32114), p. 17. La vulnérabilité des infrastructures interconnectées, la facilité d'accès à des cibles, le coût faible ou quasi – inexistant des maliciels facilitent la prolifération des dénis de services. La nouvelle génération de terroristes connectés sont autant de facteurs stimulant la montée de la menace cyberterroriste, incitant par-là les « organismes d'application de la loi et du renseignement à demander de nouveaux outils et pouvoirs », Holly PORTEOUS et Dominique VALIQUET, « La cybersécurité et la cybercriminalité : s'attaquer à une menace complexe », Le monde numérique, p. 56, disponible en ligne : http://www.parl.gc.ca/content/lop/researchpublications/cei-06-f.htm (consulté le 2 Août 2014).

[138] Voir note 126; Nicolas VERMEYS, *Virus informatiques : responsables et responsabilité,* 1ère éd., Montréal, Éditions Thémis, 2003, p. 12-24.

[139]Stratégie canadienne, préc., note 1, p. 5; Lothar DETERMANN et Karl T. GUTTENBERG, «On War and Peace in Cyberspace- Security, Privacy, Jurisdiction », **(**2013-2014**)** 41 *Hastings Const. L.Q*. 875-902.

[140]INFORMATION WARFARE MONITOR and SHADOWSERVER, *Shadows in the cloud: Investigating cyber espionage 2.0*, Toronto, 2010, p.6, [Shadows], disponible en ligne: http://www.nartv.org/mirror/shadows-in-the-cloud.pdf (consulté le 14 Avril 2014).

[141]R. DEIBERT, préc., note 6, p. 161-164.

L'implication des États [142] dans une cyberopération accroît significativement la performance des outils déployés dans le vol de données et la difficulté de contrecarrer la menace qui pèse sur l'autorité canadienne. Dans cette manœuvre, les outils de commission diffèrent selon les cibles visées (Paragraphe 1) et l'implication de l'autorité étatique n'est que présumée, faute de preuves concrètes (Paragraphe 2).

Paragraphe 1 : Les outils de commission

Le cyberespionnage étatique est une continuation de l'espionnage classique qui comporte des spécificités propres (A) tout comme le cyberterrorisme. Il est la résultante de la révolution technologique et de l'avènement du réseau, en l'occurrence d'internet, d'où il tire ses outils (B).

A. Les spécificités du cyberespionnage

Il existe une différence entre le cyberespionnage général simple et le cyberespionnage étatique qui réside dans la détermination de la cible et le procédé de l'attaque. Dans le cadre d'un cybercrime tel le *hacking* ou le sabotage informatique, les auteurs peuvent, par exemple, distiller des maliciels[143] sur une grande étendue de réseaux ou de serveurs tissant une toile [144] dans l'espoir d'attraper une proie [145] ; alors que dans le cadre du

[142] Stratégie canadienne, préc., note 1, p. 6.

[143]Il est instructif de lire à ce sujet N. VERMEYS, préc., note 138, p. 12; B. GAGNON, préc., note 8; Jason BARKHAM, «Information warfare and international law on the use of force » **(**2001-2002**)** 34 *N.Y.U. J. Int'l L. & Pol.* 57, 62-65, à la page 64, l'auteur dresse sommairement différents types de cyberattaques suivant les manœuvres utilisées.

[144]Shadows, préc., note 140, p. 8-10 et p. 27-30.

[145] Le vol des 900 Numéros d'Assurance Social par le jeune homme de 19 ans résidant à Toronto suite à la faille en ligne du programme *Heartbeat*, baptisé par les médias, *Heartbleed*, survenu en Avril 2014 au Canada est par exemple, constitutif d'un cybercrime ordinaire puisqu'il ne visait aucune infrastructure en particulier. Voir par exemple Shane DINGMAN, « How the Heartbleed bug works, and what passwords you need to change», **(**9 Avril 2014**)**, The Globe and Mail,

cyberespionnage étatique, la cible est définie à l'avance et l'attaque est dirigée vers celle-ci. Le choix de la cible permet parallèlement de définir le type de cyberespionnage[146]. Lorsque le cyberespionnage est orienté, par exemple, vers des structures étatiques ou des organismes gouvernementaux, il est de nature politique et porte des critères distincts de reconnaissance[147].

Le cyberespionnage étatique s'entend généralement de toute incursion non autorisée dans le système protégé d'un organe du gouvernement ou d'une entreprise considérée comme faisant partie d'une infrastructure essentielle[148] par le biais d'un réseau de connexion. Il est une sous-catégorie de l'espionnage classique destiné à dérober de l'information par l'infiltration d'un agent au sein d'un système informatique sécurisé. Par cette manœuvre sophistiquée exploitant un réseau électronique[149], les auteurs peuvent soutirer de l'information sensible telle que des résultats hautement confidentiels du Centre National de recherche Canada[150] par exemple.

Cette « activité illégale, clandestine ou coercitive que mène un gouvernement étranger ou ses mandataires à des fins stratégiques mondiales »[151] appelle l'utilisation d'outils ou d'opérations habituellement reconnues aux simples cybercriminels, mais qui sont, ici, destinés à des buts politiques. Cela a pour effet de créer une confusion sur la nature de l'acte et ses responsables[152], rendant très difficile la qualification de la responsabilité et restreignant le rattachement à une autorité étatique. La question de la responsabilité d'un

---

disponibleenlignehttp://www.theglobeandmail.com/technology/tech-news/explainer-what-the-heartbleed-security-bug-means-for-you/article17893562/ (consulté le 13 Avril 2014).

[146]Shadows, préc., note 140; Tracking Ghostnet, préc., note 27, p. 30-45 et p. 47-49.

[147]*Id.*

[148] L'infrastructure essentielle est une appellation définissant tout système ou actif, virtuel ou physique dont dépend le fonctionnement d'un État, J. P. GALLAND, préc., note 38.

[149] Tracking Ghostnet, préc., note 27, p. 47-49.

[150] Voir en ligne le site internet du centre :http://www.nrc-cnrc.gc.ca/fra/ (consulté le 10 Septembre 2015)

[151] Stratégie canadienne, préc., note 1, p. 24.

[152]Nart VILLENEUVE, « The "Kneber" Botnet, Spear Phishing Attacks and Crimeware », 2010, en ligne http://www.nartv.org/2010/03/01/the-kneber-botnet-spear-phishing-attacks-and-crimeware/ (consulté le 14 Décembre 2013).

État dans la manœuvre du cyberespionnage est difficile à établir puisque les principaux suspects révélés suite aux enquêtes menées sont de simples groupes qui servent de façade à l'activité illégale[153] du gouvernement.

Dans sa stratégie de cybersécurité, le Gouvernement du Canada dénonce clairement la volonté non voilée de certains États[154] de nuire aux intérêts du pays en usant de « moyens clandestins pour recueillir des informations politiques, économiques et militaires au Canada »[155] qu'ils dérobent pour avoir un certain avantage. Pour mieux comprendre la notion dans ses différentes composantes, il est utile de porter attention à la typologie des auteurs de l'acte, les buts poursuivis et les cibles visées.

L'impossible imputabilité officielle de l'acte aux agences de renseignements des États ou à leurs émissaires ne permet pas d'établir un archétype de cyberespions. Suite à la découverte d'un cyberespionnage étatique, le faisceau d'indices trouvés, qu'ils s'agissent des moyens sophistiqués utilisés ou de la sophistication de l'attaque, peut signaler l'implication d'un organe étatique mais ces indices ne peuvent pas permettre d'identifier dûment les coupables[156].

Ainsi, contrairement à la difficulté d'attribuer la responsabilité d'un cyberespionnage, en déceler le but est plus aisé. En effet, de façon générale, à partir du type de données touchés, il est facile de déduire que l'activité est menée dans l'optique de voler des informations pour obtenir un avantage économique, militaire, industriel certain sur un autre État. L'État-auteur de cet espionnage aura dès lors son capital politique renforcé ou pourra accroître sa puissance économique et/ou militaire[157].

---

[153] Lolita C. BALDOR, « L'armée chinoise emploierait des civils dans ses "unités de cyberguerre" », 19 Août 2010, La Presse Canadienne**,** Montréal.

[154] Stratégie canadienne, préc., note 1, p. 5.

[155] SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ, *Rapport 2011-2013*, 2014, p. 18.

[156] Tracking Ghostnet, préc., note 27, p. 7.

[157] *Id.*

Le choix de la cible en dit beaucoup sur le genre d'activités menées contre une instance étatique. La précision du but s'établit dans le choix de l'entité gouvernementale ou de l'entreprise visée. Lorsque la manœuvre de l'espionnage révèle une collecte exclusive de données appartenant à des infrastructures critiques, les doutes s'orientent en général vers l'implication d'un État. Les cibles du cyber espionnage sont en général les missions diplomatiques et les administrations gouvernementales, les organes de sécurité intérieure ou encore les chaires de recherche universitaires[158].

Autrement dit, la qualification de cyberespionnage se rapporte à différents éléments qui ne se précisent que dans la découverte de sa manœuvre. Aussi, « the nature and the timing of the attack, the exploit, the malware and the command and control infrastructure »[159] ne sont-ils que des aspects superficiels de l'acte, éclairant moindrement la détermination du responsable de l'acte. Ainsi, suivant l'étude *Shadows*[160], la connaissance des moyens et les outils utilisés, les données volées et leur destination sont intrinsèques à une identification véritable des contrevenants.

B. Les outils de l'activité

Le premier intérêt de l'espionnage n'est pas de porter un dommage au camp espionné, mais il vise plutôt le vol de renseignements gouvernementaux et d'informations confidentielles et militaires[161]. Il est d'autant plus dangereux que sa manifestation est insidieuse et la plupart du temps indétectable[162]. L'achèvement du but de cette manœuvre peut s'atteindre soit par l'usurpation physique d'une unité d'ordinateur, un périphérique

[158] Ces cibles sont fréquemment visés car leurs bases de données fournissent d'importantes informations utiles au développement d'une Nation et font partie des infrastructures d'un pays. Voir Fred SCHREIER, *On Cyberwarfare*, *DCAF Horizon Working Paper*, 2015, disponible en ligne http://www.dcaf.ch/Publications/On-Cyberwarfare (consulté le 5 Juin 2014).

[159] Shadows, préc., note 140, p.6.

[160] *Id.*

[161] Rapport Mandiant, préc., note 29; Études hors-séries, préc., note 11, p. 22-27.

[162] Études hors-séries, préc., note 11, p. 25.

ou un disque dur par exemple[163], soit par la pénétration non autorisée dans le réseau connecté d'une entité. Ce procédé consiste à introduire de manière directe ou détournée un maliciel dans le système d'exploitation sécurisé d'une entité afin de soutirer systématiquement des renseignements ou d'en collecter sur un plus ou moins long terme. L'opération peut consister en l'envoi d'un courriel contenant une pièce jointe infectée ou un lien hypertexte piégé au sein d'une même organisation provenant d'un membre qui travaille aussi dans cette organisation. L'ouverture de la pièce jointe ou un clic sur le lien lance une attaque couverte ou apparente sur l'ordinateur de l'employé, puis se répand dans le réseau intranet sur lequel il est connecté. Markoff et Barboza[164] mettent en lumière la manœuvre qui consiste à la propagation du virus par l'envoi d'un mail du compte de l'employé qui vient d'être infecté[165]. Ces opérations, à effet domino, sont largement facilitées par la connexion *TCP/IP* qui fonde les réseaux[166]. Le maliciel[167] comporte différents types de nuisances qui servent aux cyberespions. C'est le cas des virus informatiques[168] ou les chevaux de Troie[169] que lesdits acteurs privilégient dans leur manœuvre.

---

[163] V. PLATT, préc., note 50, p.159.

[164] John MARKOFF and David BARBOZA, « 2 China Schools Said to Be Tied to Online Attacks », 18 Février 2010, NYTimes.com, disponible en ligne: http://www.nytimes.com/2010/02/19/technology/19china.html?_r=0 (consulté le 5 Février 2014).

[165] Les thèmes de messages électroniques sont rédigés de sorte à susciter l'intérêt du/des destinataires. En général, ce sont les documents électroniques en format PPT., DOC., ou les PDF., qui sont utilisés.

[166] J. P. GALLAND, préc., note 38, p. 6.

[167] Le maliciel s'entend d'un logiciel anti-programmé destiné à nuire à un système informatique en le reprogrammant ou en s'y logeant. Voir Henri LILEN et François DAROT, *Virus et protection*, Paris, Radio, 1991, p. 12 cité par N. VERMEYS, préc., note 138, p. 13.

[168] *Id*., à la p. 15, le professeur Vermeys définit le virus informatique comme « un logiciel auto-reproductible comportant du code informatique […] pouvant infecter d'autres programmes en les modifiant ou en modifiant leur environnement, afin que l'accès à un logiciel infecté implique l'accès à une copie évoluée du virus ».

[169] Les chevaux de Troie sont des antiprogrammes qui se dissimulent dans un programme informatique valide pour y effectuer des opérations sournoises. Pour plus d'informations, voir généralement Jean François PILLOU, « Les bombes logiques » 2014, disponible en ligne : « http://www.commentcamarche.net/contents/1223-bombes-logiques#q=bombes+logiques&cur=1&url=%2F » (consulté le 7 Juin 2014); N. VERMEYS, préc., note 138, p. 19.

La manœuvre touche à la première échelle l'individu[170]. Elle peut commencer par l'envoi d'un mail ou d'un message à l'un des employés de l'entité visée, ou encore par le piratage d'un compte Facebook de l'un d'eux[171]. La réussite de ces opérations est due à la vulnérabilité des sites qui montrent une apparente sécurité à l'endroit des usagers[172].

Le cyberespionnage est facilité par l'inexistence de structures compétentes entièrement vouées à la répression du cybercrime ou de textes légaux susceptibles d'indiquer les voies d'une répression[173]. La quasi-intraçabilité et la difficile imputabilité de l'acte est de nature à faciliter les manœuvres des cyberespions[174].

Les crimes du cyberespionnage ne sont pas imputables ou, du moins, le sont très difficilement[175] en raison de la quasi-inexistence de preuves, contextuelles ou évidentes, indicatives du lieu de l'attaque et il est difficile de déterminer l'identité des attaquants.

Paragraphe 2 : La suspicion de l'implication étatique

Le cyberespionnage étatique suscite des inquiétudes de la part des gouvernements et des organismes de défense des droits humains[176] concernant surtout la pérennité économique

[170] Tom N. JAGATIC, Nathaniel A. JOHNSON et al., « Social Phishing », **(**2007**)** 50 *Communications of the ACM* 10, disponible en ligne : http://portal.acm.org/citation.cfm?id=1290958.1290968&coll=GUIDE&dl=GUIDE&CFID=74760848&CFTOKEN=96817982 (consulté le 3 Avril 2014).

[171]Ces deux exemples ne sont que des cas parmi plusieurs autres. Pour plus d'informations, voir Allen M. SMITH et Nancy Y. TOPPEL, « Case Study: Using Security Awareness to Combat the Advanced Persistent Threat », 13th Colloquium for Information Systems Security Education, 2009.

[172] R. DEIBERT, préc., note 6, p. 8.

[173]L. DETERMANN et K. T. GUTTENBERG, préc., note 137, p. 883. Les auteurs écrivent : «International law does not prohibit countries from spying abroad or punishing spies at home. »

[174]Études hors-séries, préc., note 1, p. 22-27.

[175] Shadows, préc., note 140, p.5; En outre, la quasi-implication de la plupart des États dans ce jeu d'espionnage entrave l'adoption internationale de texte de lois pénalisant l'activité, L. DETERMANN et K. GUTTENBERG, préc., note 137, p. 882-884.

[176]L. DETERMANN et K. GUTTENBERG, préc., note 137, p. 877: « Chancellor Merkel recently called for the creation of a "European data network."" Pending trade agreements have been thrown into jeopardy as

des pays et le bon fonctionnement des services publics. En dépit de la conscience du danger que cette activité représente, il persiste un manque réel de coopération continue entre les organismes étatiques et le secteur privé[177], une implication des États dans l'exécution de cet acte et, par-dessus tout, l'absence de sa pénalisation interpelle sur l'illégalité de l'acte en lui-même[178].

Il existe un nombre important d'épisodes témoignant de la dangerosité de l'activité. Ces évènements permettent de comprendre l'ampleur du phénomène et ses incidences sur le fonctionnement d'un État. L'état des lieux du cyberespionnage s'apprécie davantage avec une étude des divers cas de cyberespionnage recensés au plan national (A) et au plan international (B).

A. Les manifestations du cyberespionnage étatique au plan national

A l'instar de l'espionnage classique opéré par Jeffrey Paul Delisle[179], certaines institutions canadiennes ont, de 2009 à 2010, été espionnées par un présumé « acteur étatique »[180], vraisemblablement chinois, sans qu'une preuve sérieuse puisse être évoquée.

---

well: French President François Hollande demanded that the United States stop spying "immediately" and threatened to block negotiations […] ».

[177] V. PLATT, préc., note 50, p. 166.

[178]L. DETERMANN et K. T. GUTTENBERG, préc., note 13ç, p. 881: « So, everybody is doing it-but, is it legal? ». Nous verrons *infra*, dans le Titre II qu'il est possible de qualifier cet acte d'infraction aux termes de la Convention de Budapest.

[179] Le lieutenant Paul Delisle volait des informations pour la Russie, son jugement très récent a été rendu en Octobre 2012, le condamnant à 20 années d'emprisonnement. Il téléchargeait des dossiers contenant des secrets militaires qu'il transférait à la Russie dans un compte mail commun créé à cet effet. Les informations divulguées étant de nature stratégique secrète, leur substance n'a pas été dévoilée et les détails concernant l'espionnage n'ont pas filtré des services de renseignement canadiens. Pour plus d'informations, voir *R.* v. *Delisle*, 2012 NSPC 114; SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ, préc., note 155 ; Alison AULD, « Jeffrey Paul Delisle, Convicted Spy, Never Interviewed For More Information By Intelligence Agencies », **(**2 Août 2013**)**, *The Canadian Press*, disponible en ligne : http://www.huffingtonpost.ca/2013/02/07/paul-delisle-spy-interview-canada-intelligence_n_2640206.html (consulté le 13Avril 2014).

[180] Daphné CAMERON, « Vague de cyberespionnage: quatre cibles au Canada visées », 04 août 2011, LaPresse.ca, disponible en ligne http://www.lapresse.ca/actualites/justice-et-affaires-

Autre exemple, depuis 2009, un vaste réseau d'espionnage initié par la France et mis en place par le programme *Babar*[181] impliquait la surveillance d'institutions canadiennes dont une chaîne de média canadienne.

Ensuite, en Janvier 2011, une attaque contre les réseaux et les systèmes du gouvernement fut menée. Les pirates, supposés d'origine chinoise, ont pu accéder à ces systèmes en envoyant de faux messages dans des courriels bien définis[182].

Enfin, en Juillet 2014, le Canada a été victime d'un cyberespionnage provenant de source officielle de la Chine. Pour l'expert en sécurité Michel Juneau-Katsuya, l'attaque dirigé contre le Centre National de Recherche du Canada (CNRC) aura permis aux cyberespions de :

> « […] savoir sur quel type d'information on travaille, où on est rendus, si on est suffisamment avancés pour pouvoir voler de la propriété intellectuelle et peut-être nous damer le pion sur la scène économique et stratégique. »[183]

Ces espionnages, d'origine étatique, sont une forme d'ingérence et égratignent la souveraineté canadienne. L'accès non autorisé aux données secrètes du pays cause un déséquilibre important dans la gestion de ses affaires internes et externes. Angela Gendron et Martin Rudner expliquent que l'espionnage étatique peut :

---

criminelles/201108/04/01-4423318-vague-de-cyberespionnage-quatre-cibles-au-canada-visees.php (consulté le 15 Avril 2014).

[181] Jacques FOLLOROU et Martin UNTERSINGER, « La France suspectée de cyberespionnage », 26 Mars 2014, LeMonde.fr, disponible en ligne : www.lemonde.fr/international/article/2014/03/21/la-france-suspectee-de-cyberattaque_4387232_3210.html (consulté le 1 Avril 2014).

[182] GOUVERNEMENT DU CANADA, *Renforcer la résilience face au terrorisme : stratégie antiterroriste du Canada*, Sa Majesté la Reine du Chef du Canada, 2013, p. 20 et 24, disponible en ligne http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-fra.aspx (consulté le 15 Mars 2014) [Renforcer la résilience].

[183] Ce cyberespionnage a entraîné la coupure de toutes les connexions liant le CNRC du reste du monde. Pour plus d'informations, voir Radio-Canada avec Reuters et La Presse canadienne, « Cyberattaque chinoise contre le Conseil national de recherches », 29 juillet 2014, disponible en ligne : http://ici.radio-canada.ca/nouvelles/National/2014/07/29/001-cnrc-cyberattaque-chinoise.shtml (consulté le 30 Juillet 2014).

> « nuire aux intérêts canadiens en cas de vol de renseignements gouvernementaux stratégiques et confidentiels ou encore d'informations ou d'applications politiques et militaires; de perte de biens et de technologies à la fine pointe; de vol de propriété intellectuelle ou d'informations commerciales ou liées aux armes; d'acquisition d'entreprises qui présentent des risques pour les infrastructures essentielles stratégiques du pays; de transfert illégal des technologies à double usage. »[184]

Le Canada est un allié économique de plusieurs pays de la sous-région, il officie donc comme point de transit de nombreuses informations confidentielles. A ce titre, son système intérieur de sécurité lui donne une crédibilité sans laquelle il ne bénéficierait pas de la confiance de ses partenaires internationaux. La violation de ces paramètres et l'extraction des données effectuée lors du cyberespionnage étatique opérées par des entités étrangères expose l'intégrité de ses infrastructures à de lourds revers. En outre, les agences nationales de renseignements sont, pour la plupart, impliquées dans ce type d'espionnage en dépit de l'incidence qu'il a sur le droit des individus au respect de leur vie privée et donc à la protection de leurs renseignements personnels. Au plan international, plusieurs cyberespionnages ont également été effectués, dont plusieurs provenant de la Chine.

B. Les manœuvres du cyberespionnage étatique au plan international

La grande partie des cas de cyberespionnage recensée à l'échelle internationale n'est jamais retracée, l'identification des auteurs ne fait l'objet que de présomptions et, pendant ce temps, les actes restent impunis, le manque de coopération entre les pays et les organisations internationales sonnant comme un signal d'alarme. En cela, l'étude de ces cas permettra de réaliser le risque du phénomène face à la faiblesse des moyens de défense dont sont munies les infrastructures critiques de certains pays.

[184] Études hors-séries, préc., note 11, p. 25.

Le cas survenu au Tibet en 2007 montre que le maliciel Ghosnet, un virus polymorphe, furtif et une « bombe à retardement »[185] fut introduit dans les systèmes informatiques contaminés grâce à un fichier source auquel il était attaché. Sa propriété polymorphe lui permis de ne pas être détecté par les logiciels anti-virus implantés. La force du virus tenait dans sa capacité à prendre le contrôle des appareils connectés (webcam ou microphones). Selon l'étude menée par le groupe *SecDev,* ce vaste réseau d'espionnage s'est étendu à plus de 103 pays collectant les données de 1295 ordinateurs. Selon Symantec[186], les mails ciblés piégés provenaient à 28,2% de la Chine, à 21,1% de la Roumanie et à 13,8% des États-Unis ; envoyés à « des experts policiers, à des missions diplomatiques, à des chercheurs universitaires et des activistes des Droits de l'Homme »[187].

L'implication d'un État dans cette affaire semble être l'hypothèse la plus vraisemblable au su des maliciels sophistiqués, de la technologie à la fine pointe utilisée et des procédés d'introduction ingénieux de ces maliciels qui dépassaient les simples capacités habituellement reconnues aux criminels de base. Suite à des investigations menées par le Centre des études internationales Munk de Toronto[188], il fut découvert que l'activité émanait de la Chine, précisément de l'île de Hainan[189]. Sans surprise, celle-ci nia toute implication dans cette affaire[190].

---

[185] N. VERMEYS, préc., note 138, p. 17.

[186] SYMANTEC, *The Nature of Cyber Espionage: Most Malicious File Types Identified and Encrypted Spam from Rustock*, Message Labs Intelligence, 2010, disponible en ligne : http://www.messagelabs.com/mlireport/MLI_2010_03_Mar_FINAL-EN.pdf (consulté le 1 Avril 2014).

[187] *Id.*

[188] Tracking Ghostnet, préc., note 27, p. 17.

[189] Philippe CROUZILLACQ, « GhostNet, le cyber-espion qui venait de Chine», disponible en ligne : www.01net.com/editorial/500430/ghostnet-le-cyber-espion-qui-venait-de-chine/ (consulté le 14 Mars 2014) ; Tracking, préc., note 27, p. 12-14.

[190] Pour Ronald DEIBERT et Nestor ARELLANO, l'absence de liens directs laissent à croire que le gouvernement chinois pourrait être impliqué, mais seulement en partie, puisque toutes les institutions espionnés ne semblaient pas avoir d'intérêts géostratégiques avec le pays. Voir généralement Ronald DEIBERT and Nestor ARELLANO, « U of T researchers uncover spy network», (2009) 25 *Computer World Canada* 7, disponible en ligne: http://search.proquest.com/docview/219926554?accountid=12543 (consulté le 4 Avril 2014).

Toute activité de cyberespionnage laisse floues les pistes d'investigations pour dénicher le coupable. Dans le cas présent, en dépit de la désignation claire des intérêts motivant ce cyberespionnage, l'attribution à un État précis demeure incertaine. Ainsi, les chercheurs chargés d'étudier ce vaste espionnage se sont vus refuser l'accès à certaines informations qui auraient pu donner des pistes[191]. En dépit du fait que le but de l'opération semblerait être un vol d'informations confidentielles, il demeure quelque peu flou puisqu'il n'est pas possible de connaître exactement les données qui ont été copiées. Cela est d'autant plus compliqué que le virus a infecté plusieurs postes à travers plusieurs pays, écartant la possibilité de déterminer la cible précise de l'activité.

En 2010, les infrastructures iraniennes ont été infestées par un ver informatique, le *Stuxnet* qui annonce une nouvelle ère et une nouvelle dimension d'espionnage cybernétique avec des ascendances de sabotage (modification de fichiers enregistrés sur un poste ou conservé dans un serveur) : le cybersabotage[192]. Le ver était calibré pour nuire exclusivement aux infrastructures critiques. Le calibrage sophistiqué de ce virus impliquait des spécificités géographiques et des installations industrielles bien précises, à savoir les pipelines de pétrole et des installations nucléaires[193].

Dans cette affaire, la cible de l'espionnage est déterminée et l'attaque a pour objectif principal de collecter les données relatives aux infrastructures critiques et de saboter ces installations. Ce n'est qu'en 2013 que des indices ont conduit à identifier les États-Unis comme les principaux suspects de l'attaque[194].

---

[191] Tracking Ghosnet, préc., note 27, p. 16-44.

[192] William J. BROAD et David E. SANGER, « Worm aws perfect for sabotaging centrifuges », 18 Novembre 2010, NewYork Times, cité par G. KERSCHICHNIG, préc., note 33, p. 69.

[193] David E. SANGER, « Iran fights malware attacking computers », 25 Septembre 2010, New York Times.

[194] LeMonde.fr ; « Etats-Unis : un ex-général soupçonné de fuites sur une cyberattaque contre l'Iran », (28 Juin 2006), en ligne http://www.lemonde.fr/ameriques/article/2013/06/28/etats-unis-un-ex-general-soupconne-de-fuites-sur-une-cyber-attaque-contre-l-iran_3438286_3222.html (consulté le 17 Août 2014).

Ensuite, depuis 2002, les données téléphoniques de la chancelière allemande Angela Merkel étaient collectées de façon continue par les services secrets des États-Unis[195]. Plusieurs autres pays de l'Union Européenne ont également subis cet espionnage jusqu'aux dénonciations faites par Edward Snowden[196]. En 2012, ce fut au tour de la France d'être espionnée, supposément par les États-Unis[197] qui aurait accéder au système informatique du gouvernement via le compte Facebook de l'un de ses employés[198] et y aurait introduit un maliciel pour copier des données informatiques confidentielles ayant trait à la stratégie militaire du pays. L'attaque a pu être retracée par l'identification du

[195]LeMonde.fr, « Les États-Unis auraient espionné le téléphone de Merkel dès 2002 », 20 Octobre 2013, disponible en ligne : http://www.lemonde.fr/technologies/article/2013/10/26/les-etats-unis-auraient-espionne-le-telephone-de-merkel-des-2002_3503620_651865.html (consulté le 10 Janvier 2014). Suite à cet espionnage la chancelière a réclamé la signature d'un accord de non-espionnage entre les pays de l'Union Européenne et entre l'Allemagne et les États-Unis, Lapresse.ca, « Espionnage: Merkel n'a pas à s'inquiéter, assure Obama », 18 Janvier 2014, disponible en ligne : http://www.lapresse.ca/international/dossiers/sous-surveillance/201401/18/01-4730087-espionnage-merkel-na-pas-a-sinquieter-assure-obama.php (consulté le 16 Mars 2014).

[196] LeMonde.fr, « La NSA aurait mis sur écoute 35 "leaders internationaux" », 2 Octobre 2013, disponible en ligne : http://www.lemonde.fr/technologies/article/2013/10/24/un-document-montre-que-la-nsa-a-surveille-35-leaders-internationaux_3502675_651865.html (consulté le 10 Janvier 2014).

[197] Les soupçons pesant sur les États-Unis ont également été nourris par la marque de fabrique du virus dont la conception a requis un investissement considérable de la part de la NSA et des services de renseignements israéliens : « Le code malveillant utilisé affiche, en effet, les mêmes fonctionnalités qu'un ver informatique extrêmement puissant, baptisé Flame, identifié à la fin du mois de mai par une grande société russe d'antivirus, Kaspersky. "Très perfectionné, il peut collecter les fichiers présents sur une machine, réaliser des captures d'écran et même activer le microphone d'un PC pour enregistrer les conversations, explique Vitaly Kamluk, spécialiste du sujet chez cet éditeur. Sa conception a demandé beaucoup d'argent et des moyens humains que seul un grand pays est en mesure de mobiliser." Ou même deux : selon la presse anglo-saxonne, le ver aurait été créé par une équipe américano-israélienne, car il devait viser initialement des pays du Moyen-Orient (Iran, Égypte). Autre élément à charge : tel un peintre reconnaissable à son trait, un virus porte les marques du savoir-faire de son auteur […]. » [Nous soulignons]. Voir Charles HAQUET et Emmanuel PAQUETTE, « NSA: les Américains étaient-ils à l'origine de l'espionnage de l'Élysée en 2012? », **(**20 Novembre 2012**)**, en ligne; http://lexpansion.lexpress.fr/high-tech/nsa-les-americains-etaient-ils-a-l-origine-de-l-espionnage-de-l-elysee-en-2012_1340421.html (consulté le 5 mai 2013).

[198] Philippe BERNARD et Corine LESNES, « Une cyberattaque américaine aurait visé l'Élysée », 22 Novembre 2012, LeMonde.fr, disponible en ligne : http://www.lemonde.fr/international/article/2012/11/22/une-cyberattaque-americaine-aurait-vise-l-elysee_1794150_3210.html (consulté le 20 Octobre 2013).

virus utilisé[199]. Les américains continuent cependant de démentir leur implication dans cet espionnage en dépit du faisceau de « présomptions » existant[200].

Enfin, en Août 2014, le monde découvrait le vol de 4,5 milliards mots de passe, étendu sur tout le globe, opéré par la Russie[201].

Les menaces de cyberespionnage sont une grande préoccupation nationale et internationale du fait des conséquences qu'elles peuvent avoir sur la fiabilité des institutions d'un pays, le respect de la confidentialité des renseignements, la garantie de la sécurité de ses infrastructures.

Ces cas de cyberespionnage ne sont pas les seuls survenus mais ont l'avantage de démontrer l'existence du phénomène et la nécessité d'éclaircir sa qualification pénale au plan international[202]. Les principaux défis que pose le cyberespionnage étatique à la communauté internationale se résument en des points bien précis, à savoir 1) l'impossible imputabilité de ce crime à un État en raison de l'absence de preuves tangibles et 2) le défaut international de qualification de l'acte qui rend incertaine son caractère illégal.

En définitive, les MSP que représentent le cyberespionnage étatique et le cyberterrorisme, parrainé par les États ou non, sont dues à l'ubiquité du cyberespace et appellent donc la mobilisation de la communauté internationale pour dresser un cadre de lutte efficace afin de garantir la pérennité des institutions étatiques. Conscient du péril auquel exposent ces dérives, le gouvernement canadien a élaboré des corps de règles visant à prévenir le vol de données informatiques et tout dommage pouvant être causés à ses infrastructures critiques et à sa stabilité sociale.

---

[199] *Id.*

[200] *Id.*

[201] LeMonde.fr avec AFP, « Des pirates informatiques russes auraient volé plus d'un milliard de mots de passe », 6 Août 2014, disponible en ligne : http://www.lemonde.fr/pixels/article/2014/08/06/des-pirates-informatiques-russes-auraient-vole-plus-d-un-milliardv-de-mots-de-passe_4467212_4408996.html (consulté le 6 Août 2014).

[202] La qualification de cet acte selon la Convention de Budapest sera abordée *infra*, Titre II.

Chapitre 2 : Les mécanismes internes et régionaux de protection des infrastructures critiques

La notion de sécurité est indissociable de la notion de risque[203] puisqu'il existe entre les deux, un lien d'interdépendance. Sans risque, nul besoin d'établir des paramètres de sécurité[204]. Ainsi, du point de vue de Karim Benyekhlef et Nicolas Vermeys, la sécurité est avant tout « garante du risque que l'on encourt »[205]. A l'échelle étatique, ce souci de prévention et de protection s'assimile à la notion de sécurité nationale dont la préservation représente un enjeu majeur pour le gouvernement canadien. C'est à cette fin que celui-ci a mis en place des organes de contrôle et de prévention chargés de la protection des infrastructures essentielles, qui incarnent, par ailleurs, le centre névralgique des vulnérabilités menaçant la stabilité étatique. En effet, les infrastructures essentielles sont considérées comme des actifs de l'État[206] qui assurent l'approvisionnement de la société en ses besoins et lui permettent de « survivre et de prospérer »[207]. Pour cause, au sein de chacune d'elles sont logées d'importantes informations dont l'origine et/ou le contexte leur donne une valeur incontournable et vitale. De fait, afin de garantir la protection de ces informations indispensables à la bonne marche des infrastructures essentielles[208], le gouvernement canadien a établi certaines dynamiques institutionnelles (Section 1). C'est dans cette logique que le SP a élaboré et publié sa stratégie de cybersécurité[209] en 2010. D'une part, celle-ci aborde en des points précis les grandes lignes d'une lutte efficace au niveau de toutes les institutions canadiennes faisant partie des infrastructures

[203] Karim BENYEKLEFF et Nicolas VERMEYS (dir.), *Le droit à la sécurité la sécurité par le droit*, Montréal, Éditions Thémis, 2010, p. 3.

[204] *Id.*, p. 4.

[205] *Id.*, p. 3.

[206] J. P. GALLAND, préc., note 38.

[207] Robert A. MILLER and Irving LACHOW, « Strategic fragility: Infrastructure Protection and National security in the information age », **(**Janvier 2008**)** 2 *Defense horizons* 59.

[208] G. KERSCHICHNIG, préc., note 27, p. 42.

[209] Stratégie canadienne préc., note 1.

essentielles[210]. D'autre part, elle aborde la question essentielle de la défense passive et active mise en place au sein de l'organisation gouvernementale. Outre ces dispositions internes de cybersécurité, le gouvernement travaille également en collaboration avec d'autres pays. Ces ententes constituent des apports aux mécanismes régionaux et internationaux de cybersécurité (Section 2).

Section 1 : Les dynamiques institutionnelles

De façon sommaire, le renseignement de sécurité s'entend de toutes les informations vitales au fonctionnement interne de l'appareil étatique et qui définissent les paramètres exécutés pour garantir une quiétude et une certaine stabilité nationale[211]. Un tel renseignement peut également être identifié en fonction de son contexte ou de la compétence reconnue à une institution de le collecter, de l'utiliser ou encore de le divulguer. Selon le contexte, les renseignements de sécurité sont « des informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces contre la sécurité du Canada »[212]. Tout renseignement personnel qui fait partie d'une enquête[213] menée par la sécurité interne de l'État, que ce soit à l'échelle nationale ou dans le cadre d'une coopération internationale devient alors un renseignement de sécurité.

La circulation de ce type de renseignement sur le réseau constitue dès lors une vulnérabilité du gouvernement en raison de la nature du renseignement de sécurité

[210] Ces infrastructures sont composées de différents corps de recherche chargés de leur bon fonctionnement et de leur bon rendement. L'importance de ces infrastructures se rapporte aussi aux informations qu'elles véhiculent ou qu'elles créent.

[211] BIBLIOTHEQUE DU PARLEMENT, préc., note 128.

[212] *Loi sur le service canadien du renseignement de sécurité,* LRC 1985, c C-23, art 12 (ci-après *LSCRS*).

[213] La *Loi sur la protection des renseignements personnels* définit comme « *enquête* » les activités liées à « la détection, à la prévention et à la répression d'un crime », « aux activités destinées à faire respecter les lois fédérales ou provinciales » ou à celles soupçonnées de constituer des menaces envers la sécurité du Canada […] », mais ce sont aussi ces renseignements qui seraient susceptibles de nuire au bon déroulement d'une enquête. *Loi sur la protection des renseignements personnels*, L.R.C. (1985), c. P-21.

intérieure (Paragraphe 1). La vitalité de ces éléments conduit le gouvernement à dédier des corps de contrôle et d'application de la loi à son exclusive protection dans sa stratégie de cybersécurité nationale (Paragraphe 2).

Paragraphe 1 : La nature du renseignement de sécurité intérieure

Le renseignement de sécurité intérieure peut être identifié selon l'organisme d'où il émane ou selon le contexte de sa collecte et/ou de son utilisation. Il peut donc être purement critique[214] ou contextuel (A). La plupart des renseignements de sécurité sont intégrés dans la nomenclature des infrastructures essentielles, ce qui les rend plus vulnérables, d'autant plus qu'elles ont un fort degré d'interdépendance (B).

A. L'information purement critique et l'information contextuelle

Substantiellement, l'information critique est reliée au fonctionnement d'une infrastructure essentielle, qu'elle soit le pur fruit de recherches scientifiques ou qu'elle définisse les paramètres de fonctionnement de l'opérabilité et du contrôle de son système d'exploitation. Il existe plusieurs infrastructures essentielles qui concourent au fonctionnement de la structure étatique et sociale dont quatre sur les dix recensés par le gouvernement canadien [215] , ont une certaine prévalence [216] : le transport, la télécommunication, les finances et l'énergie[217].

[214] Les termes exacts employés sont : « critical information infrastructure» pour désigner les informations dont dépendent les infrastructures critiques. Voir généralement G. KERSCHICHNIG, préc., note 33, p. 40-44.

[215] Études hors-séries, préc., note 11, p. 7-14.

[216] *Id.*, voir note 16.

[217]La prévalence de ces infrastructures critiques ressort d'études effectuées par le gouvernement canadien. Voir en général Études hors-séries, préc., note 11.

. Le transport

Les transports sont une pièce indispensable au mécanisme global de fonctionnement de la machine étatique. Le secteur comprend le transport routier, ferroviaire, aérien et maritime. *Transport Canada*[218], dont les recettes de 17 de ses aéroports étaient de 12,2 millions, verrait aujourd'hui cet actif chuter si une faille majeure était découverte dans son système. Il est effectivement déjà arrivé qu'un bug informatique paralyse un aéroport causant d'importantes pertes économiques. C'est le cas de l'aéroport de Los Angeles dont le système informatique de la base de contrôle aérien ont connu une panne en Avril 2014[219]. Les pertes pourraient également toucher le transport maritime si une cyberattaque le visait. Ainsi, le coût destiné à la sécurisation de l'infrastructure (soit 1,8 M$ alloué en 2013 par le Programme de contribution pour la sécurité nautique (PCSN))[220], se verrait triplé. De même, le taux d'exportation, chiffré à 11,6%[221], pourrait s'en voir diminué.

. Les télécommunications

Ce secteur est avant-gardiste des dernières innovations technologiques dans la plupart des autres secteurs d'activités et est une plateforme de liaison entre les différents acteurs y intervenant. Les nouvelles technologies de l'information et de la télécommunication comprennent les protections des différentes connexions dont l'internet et les bases de données, les systèmes de télécommunications des résidences privées et des entreprises, les satellites et la radio. La vulnérabilité des structures de protection des innovations technologiques demeure une question prioritaire. Les risques dans ce secteur sont très importants. Il suffit de prendre le secteur de la télécommunication mobile pour se rendre

[218]GOUVERNEMENT DU CANADA, *Les Transports au Canada 2012*, Canada, 2013, p. 12.

[219]AFPQC2, « Un bug informatique du contrôle aérien à Los Angeles perturbe le ciel américain », 30 Avril 2014, disponible en ligne : http://quebec.huffingtonpost.ca/2014/04/30/un-bug-informatique-du-co_n_5243588.html (consulté le 13 Octobre 2014). Cet incident a causé d'importants retards et plusieurs avions furent redirigés vers d'autres pistes. Le bug aura certainement baissé la fréquentation de l'aéroport qui était de 66 millions de passagers en 2013.

[220]GOUVERNEMENT DU CANADA, *Les Transports au Canada 2013*, Canada, 2014, à p. 6 :« Le transport aérien est l'un des plus bénéfiques à l'économie canadienne est a rapporté aux recettes du budget 2012 – 2013, un total de 14,0M$ ». En cas de bris, cette recette diminuerait substantiellement.

[221]*Id.*

compte des vulnérabilités des systèmes de protection informatique. Prenons un exemple d'une technologie couramment utilisée au sein des ministères, l'iPad. Selon un rapport rédigé par le Centre de la sécurité des télécommunications (ci-après CSTC), l'utilisation des iPad [222] au sein des institutions ministérielles comporte des risques élevés de cyberattaques via le navigateur Safari. Ces risques sont d'autant plus élevés lorsqu'il s'agit d'un accès illégal à un système informatique du gouvernement qui permet d'accéder à des renseignements critiques[223].

. L'énergie

Le secteur énergétique, à cause de son importance, est une mine de vulnérabilités. Il permet la production, le traitement et l'emmagasinage du pétrole et du gaz, la fourniture de l'électricité, la transmission, la distribution de l'électricité ainsi que la production d'énergie nucléaire. Il dessert clairement tous les secteurs d'activités nationales et représente donc un atout économique important[224]. L'entreprise Hydro-Québec possède son propre réseau de distribution dont les paramètres de fonctionnement représentent à eux seuls des renseignements de sécurité puisque l'institution dessert tous les autres secteurs critiques, que ce soit le transport, les télécommunications ou les finances. Il en

[222] CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS, *Rapport ITSB-65*, **(**Juillet 2013**)**, en ligne https://www.cse-cst.gc.ca/fr/node/234/html/9892 (consulté le 6 Octobre 2014).

[223] *Id*. Le rapport mentionne en autres sortes de faiblesses recensées pour l'utilisation des iPad au gouvernement, l'impossibilité de définir le type de réseau afin que des mesures de sécurité soient automatiquement mises en place comme c'est le cas pour les postes de travail et les ordinateurs portables qui permettent une installation de mesures informatiques de sécurité. Cette limitation est essentiellement due aux fonctions intégrées du système d'exploitation IOS. Le rapport dresse par ailleurs d'intéressantes alternatives afin de limiter les risques mais celles-ci ne sont pas infaillibles. C'est le cas des risques que comportent les maliciels. En effet, ceux-ci peuvent être intégrés par le téléchargement des diverses applications puisque l'iTunes ne contrôle pas le code des applications mais juge uniquement le contenu inacceptable. A ce risque, le CST émet cette stratégie : « Il est recommandé que les ministères établissent un programme permettant de s'assurer que les versions les plus récentes des logiciels sont installées sur tous les dispositifs Apple ». Cependant le risque persiste puisqu'il faut alors s'assurer que le contrôle qu'Apple opèrera sur les versions récentes de chacune des applications.

[224]Études hors-séries, préc., note 11, p. 10-11.

est de même pour des entreprises telles que Union Gas ou encore Enbridge Gas qui contribuent à la croissance de l'économie canadienne[225].

. Les finances

Le secteur des finances est aussi un actif très important de l'État. Avoir connaissance ou saboter les prévisions du marché boursier canadien par exemple, ou encore bloquer la mise sur le marché d'un quelconque prototype technologique peut avoir une incidence sur le fonctionnement des services publics ou sa rentabilité. En effet, une simple panne informatique peut causer d'importants dommages à une banque. C'est le cas de la Banque nationale qui avait subi, du fait de simples maladresses informatiques, une panne qui a causé des préjudices à de plusieurs clients[226]. De même, dévoiler des prévisions financières peut amener le Canada à perdre un important marché international. Sachant que le secteur financier inclut, du côté du secteur privé, les diverses opérations bancaires, les services financiers ou les opérations boursières; et, du côté du gouvernement, ce sont les prévisions budgétaires qui composent le secteur financier canadien, soit environ « 20 % du PIB du Canada en 2011 »[227]. Les infrastructures financières dépendent énormément des autres infrastructures, notamment celles de l'énergie qui permet l'alimentation en électricité des quelques 18 000 guichets automatiques implantés sur tout le territoire[228].

Par ailleurs, tel que mentionné plus haut, le renseignement de sécurité peut être défini par le contexte. Ainsi, dans la décision rendue par la Cour Fédérale dans l'affaire *Ruby c.*

---

[225] Union Gas fait partie du palmarès des 100 meilleurs employeurs canadiens durant trois années successives et EnbridgeGas est un distributeur internationale de gaz naturel. Ces deux institutions sont en collaboration avec Gaz métro dans le but de fournir du gaz à tout l'Est canadien. Pour plus d'informations, voir en ligne http://www.corporatif.gazmetro.com/corporatif/communique/fr/html/3800114_fr.aspx?culture=fr-ca (consulté le 4 Décembre 2014).

[226] *Bergeron* c. *Banque Royale du Canada*, 2006 QCCS 5226, en ligne https://www.canlii.org/fr/qc/qccs/doc/2006/2006qccs5226/2006qccs5226.html (consulté le 5 Décembre 2014).

[227] Renforcer la résilience, préc., note 182, p. 12.

[228] *Id.*

Canada[229], le Service Canadien du Renseignement de Sécurité (ci-après, SCRS) invoqua en partie les articles 21 et 22 de la *Loi sur la Protection des Renseignements Personnels*[230] (ci-après LPRSP) pour s'opposer à la divulgation d'un renseignement personnel, fruit d'une enquête préalable[231], le qualifiant de « *renseignement délicat* »[232]. L'institution a également mis l'emphase sur les conséquences que la communication de ce renseignement pourrait engendrer[233]. Dans le cas présent, l'implication de M. Ruby dans une enquête menée par le SCRS a systématiquement changé la nature de ses renseignements personnels en renseignements de sécurité puisque la personne concernée était soupçonnée « pour des motifs raisonnables, de se livrer à des activités directement liées à l'espionnage ou au sabotage et de nature hostile ou préjudiciable au Canada »[234].

Les renseignements de sécurité liés à une infrastructure critique permettent de les identifier et définissent les paramètres de fonctionnement qu'ils fondent. Ils conditionnent

---

[229] *Ruby* c. *Canada (Solliciteur Général),* [1996] 3 CF 134, disponible en ligne http://www.canlii.org/fr/ca/cfpi/doc/1996/1996canlii4052/1996canlii4052.html (consulté le 2 Avril 2014).

[230] *Loi sur la protection des renseignements personnels*, L.R.C. (1985), c. P-21.

[231] Robert MACEWAN, Directeur général de l'antiterrorisme au SCRS dans son affidavit du 18 Février 1993, dans *Ruby* c. *Solliciteur général*, préc., note 229.

[232] Autrement dit, il s'agissait d'informations touchant à d'éventuelles activités subversives, révélant peu ou en partie des détails de négociations diplomatiques, ayant un rapport poussé avec la défense du pays ou encore, visant des banques de données renfermant des renseignements. Dans ses motivations, l'Honorable juge Simpson ne fait cependant pas de spécifications sur la nature de ces systèmes de collecte de renseignements dressant un cadre général libre d'Interprétation. Cependant, dans notre étude, il sera exclusivement question de banque de données gouvernementales destinés à la protection des intérêts nationaux ou recensant des informations critiques.

[233] La divulgation de ces renseignements serait de nature à nuire à la collaboration entre l'agence de renseignement qui a aidé à obtenir les informations et le service de renseignement canadien.

[234] Le rejet de la communication des renseignements au requérant était d'autant plus motivé par le souci de conserver une bonne relation de confiance avec les coopérants étrangers qui favorisaient la circulation de l'information et la bonne tenue des enquêtes. En effet, les services de sécurité, dans leurs activités et enquêtes sur des crimes majeurs reliés au réseau internet, ont besoin d'informations qui sont disséminés dans différents pays. Ils doivent, de ce fait, respecter la politique de protection de la confidentialité de la source et du contenu de l'information; la fuite d'une information confidentielle pouvant entraîner un bris de confiance. Voir à cet effet Affidavit MacEWAN, préc., note 229, ou encore, Affidavit John M. FRASER dans *Ruby* c. *Canada*, préc., note 229, p.14 ou Affidavit Margaret Ann PURDY, ancienne directrice générale de l'antiterrorisme, 31 Octobre 1994, affidavit François M. J. Hummel, ancien surintendant à la GRC, 4 Novembre 1994, affidavit du Professeur John M. Fraser, ancien directeur général à la direction du renseignement extérieur au Ministère des affaires extérieures, tous ces affidavits sont contenues dans *Ruby* c. *Canada*, préc., note 229, p.11.

surtout la santé économique et financière de cette structure en raison de son employabilité, de l'exportation qu'elle favorise et de l'appel aux investissements extérieurs qu'elle permet de garantir. La vulnérabilité de ces renseignements est intrinsèque à leur importance dans une société aussi connectée que le Canada. Celle-ci est exacerbée par leur interdépendance au réseau et entre elles. La protection du renseignement de sécurité est un enjeu de la cybersécurité canadienne dans laquelle s'inscrit l'interdépendance des infrastructures.

B. L'interdépendance des infrastructures

Les infrastructures essentielles sont dépendantes les unes des autres suivant que cette dépendance se fonde sur un « lien physique, géographique ou cybernétique »[235] ou encore sur la base d'un réseau[236]. Elles sont le plus à risque lorsqu'il y a une dépendance réseau-service qui comporte les paramètres de fonctionnement de l'une ou l'autre des infrastructures connectées[237]. On parle alors de dépendance structurelle qui peut entraîner une vulnérabilité de la même nature[238]. Beaucoup d'infrastructures critiques ont une dépendance structurelle nécessaire à leur mode de fonctionnement, en l'occurrence celle basée sur le Système intégré d'Acquisition et de Contrôle des Données (ci-après SCADA)[239]. Ce système de gestion et de contrôle opère dans la plupart des secteurs vitaux d'une société raccordant des réseaux de production sur une échelle internationale[240].

---

[235] Études hors-séries, préc., note 11, p. 14.

[236] J.P. GALLAND, préc., note 38, p. 12.

[237] *Id.*

[238] J.-F. GLEYZE, *La vulnérabilité structurelle des réseaux de transport dans un contexte de risques*, Thèse de doctorat, Paris VII, Université Denis Diderot, 2002 cité par J.P.GALLAND, préc., note 38, p. 14.

[239] La notion sera abordée *infra*, 48-51.

[240] Toute infrastructure ou une simple structure présent ou non sur le territoire pourrait constituer une infrastructure essentielle. Galland établit une catégorisation multiple sur la base de la menace ou du risque que représenterait la structure ou le secteur au cas où elle serait sous l'emprise de puissances étrangères ou de groupes terroristes. J.P. GALLAND, préc., note 38, p. 12.

Son unicité et sa connexion au réseau internet le rendent très vulnérable[241]. Ceci est d'autant plus problématique qu'il est utilisé au Canada [242] par les industries de production[243], dans la production de l'énergie ainsi que pour les forages. La protection de ces industries est en partie assurée par la politique canadienne de sécurité nationale : « Protéger une société ouverte »[244].

Cette protection des infrastructures essentielles[245] représente un enjeu qui va au-delà de leur simple fonctionnalité et de leur rôle dans la prospérité économique d'un État et d'une Nation. Sa mise en œuvre est en effet conditionnée par la fiabilité de tous les réseaux qui lient ces différentes structures et les systèmes de contrôle dont elles dépendent. Les industries de production des différents secteurs utilisant le SCADA ont plus de facilités à contrôler et à commander le processus de production et de distribution. Les exploitants de ce système aident plus rapidement à la fourniture de services publics à la population et l'intègre à une grande partie des réseaux canadiens et dans beaucoup d'autres pays. Son

[241]Alvaro A. CARDENAS, Tanya ROOSTA et Shankar SASTRY, « Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems », **(**2009**)**, *Ad Hoc Networks Elsevier*, p. 2-7. Dans cet article, les auteurs mettent en scène différents scénarios de dommages causés au système par l'exploitation de ses failles. Concernant les attaques extérieures via son réseau TCP/IP, ils donnent cet exemple : « Spoofing attack: In this attack, a system entity illegitimately assumes the identity of an authorized system entity. If sensor nodes are not authenticated properly, this attack is very easy to launch. The lack of proper device authentication was the reason the attack on the sewage system at Maroochy Shire [3] was successful. Attack class: final; if an attacker can spoof a legitimate node in the network, then it can send arbitrary values on its behalf and compromise our system integrity », p. 5.

[242]Études hors-séries, préc., note 11, p. 15.

[243] Les industries de production impliquant un nombre important d'acteurs privés implique une décentralisation du contrôle des normes de sécurité adéquates. Voir plus généralement COMMISSION DES COMMUNAUTES EUROPEENNES, *Livre vert sur un programme européen de protection des infrastructures critiques*, 1ère éd., COM final, 2005, p. 9.

[244] GOUVERNEMENT DU CANADA, BUREAU DU CONSEIL PRIVÉ, *Protéger une société ouverte: la politique canadienne de sécurité nationale*, Sa Majesté la Reine du Chef du Canada, 2004, disponible en ligne : http://www.bcp.gc.ca/docs/information/publications/aarchives/natsec-secnat/natsec-secnat-fra.pdf (consulté le 12 Mars 2014) [Protéger une société ouverte].

[245]Pour qu'elle soit essentielle, il faut que l'infrastructure produise des « extrants essentiels »[245] à la bonne marche des autres secteurs et leur soit vitales. Pour plus d'informations, GOUVERNEMENT DU CANADA, préc., note 182, p. 54.

utilité et son efficacité exposent cependant à des vulnérabilités qui peuvent entraîner des réactions à la chaîne en cas de sabotage[246].

A l'échelle des industries, « extrants essentiels » du fonctionnement étatique, ce sont les Industrial Control Systems (ICS), des systèmes de gestion de production et de l'opérabilité des processus de fonctionnement qui relient les différentes infrastructures[247]. Les ICS fonctionnent sur la base de deux programmes : le SCADA et le Système de Contrôle Distribuée (Distributed Control System, ci-après DCS) [248] . Leur récente connexion[249] à l'internet a conduit à agrandir les failles que comportaient déjà le SCADA, créant depuis lors des interdépendances entre les différentes structures intégrant le programme[250]. Une malencontreuse manipulation de ces programmes, une insertion d'un code erroné ou une interruption de service a un effet immédiat sur le bon fonctionnement des infrastructures essentielles[251].

---

[246]Aunshul REGE, « Industrial control systems and cybercrime », dans T. J. HOLT, préc., note 60, p. 194 ; Le SCADA est une cible très probable du cyberterrorirsme car, au nombre des dégâts qu'une défaillance de ce système pourrait causer, il y a l'interruption des industries de production atteint, ce qui entraînerait une perte très lourde pour l'économie du ou des pays victimes, et une coût faramineux. Une telle attaque est susceptible d'entraîner des pertes en vies humaines dépendamment de l'ampleur de l'attaque. Voir Giampiero GIACOMELLO, « Bangs for the buck: A cost-benefit analysis of cyberterrorism», **(**2004**)** 275 *Studies in Conflict & Terrorism* 387-408, disponible en ligne: http://search.proquest.com/docview/60707526?accountid=12543 (consulté le 17 Octobre 2014).

[247] Le SCADA collectionne les données émises par une infrastructure et assure le suivi des procédures et la bonne marche des opérations, sur un périmètre géographique très étendue. Le DCS, quant à lui effectue juste un contrôle sur une zone géographique bien définie. Voir plus généralement A. REGE, préc., note 246.

[248] Pour plus d'informations sur les ICS et le SCADA, voir Robert RADVANOVSKY et Allan MCDOUGALL, préc., note 38, p. 235-241.

[249] Ce n'est qu'après 1990 que les ICS furent reliés l'internet afin d'augmenter leur capacité et leur rapidité.

[250]Un exemple de la vulnérabilité de ce système de contrôle s'est manifesté dans le cas de Maroochy en Australie où un homme a réussi à accéder au système SCADA et a déversé des eaux dégoûts dans des cours d'eau. Voir Alvaro A. CARDENAS, Tanya ROOSTA et al., préc., note 241, p. 2.

[251] Au Canada, le système d'hydraulique utilise le SCADA qui permet de suivre et de vérifier le bon fonctionnement des machines et de s'assurer de l'absence de failles dans le système. Ce système est également utilisé dans plusieurs pays pour assurer le bon fonctionnement de la production au sein de structures étatiques. Sa liaison avec l'internet l'expose dorénavant aux risques de cyberattaques qui minent tous les réseaux cyber-reliés, augmentant de façon significative les vulnérabilités des infrastructures essentielles du Canada. Voir généralement IBM, *SCADA Security Solutions*, disponible en ligne : http://www-935.ibm.com/services/us/en/it-services/scada-security-solutions.html (consulté le 14 Avril 2014); Robert RADVANOVSKY et Allan MCDOUGALL, préc., note 38, p. 241.

Les institutions gouvernementales, conscientes de ces enjeux relatifs à la vulnérabilité de ses infrastructures critiques, à la sensibilité des renseignements de sécurité et aux cybermenaces pesant sur leur intégrité, ont adopté une série de mesures, à la fois législatives et structurelles afin d'atténuer les risques encourus et de renforcer ses infrastructures. A cette fin, la stratégie de cybersécurité canadienne définit un cadre institutionnel en charge de la défense passive et active du numérique.

Paragraphe 2 : La mise en exécution de la stratégie

Dans le registre de la lutte contre le cyberterrorisme ou le cyberespionnage étatique, la stratégie de cybersécurité canadienne, bien qu'émanant d'un ministère[252], délègue à des corps institutionnels des charges exclusives ou non de prévention et de protection cybersécuritaire suivant un organigramme précis (A). Le gouvernement canadien a également mis en place des politiques de cybersécurité encadrant la défense passive et active contre les cyberintrusions, définissant par-là, un cadre technique global (B).

A. Organigramme des structures vouées à la protection des renseignements de la sécurité et des infrastructures critiques

Comme mentionné plus haut, la considérable place du renseignement de sécurité dans la protection des intérêts canadiens appelle la présence d'organismes du renseignement de sécurité. Au Canada, il existe plusieurs institutions fédérales qui travaillent à la protection des actifs de l'État. Trois institutions principales ont la charge d'assurer le renforcement de la cybersécurité canadienne. Ce sont le CSTC, le SCRS et la Gendarmerie Royale du Canada (ci-après GRC).

[252]Selon Benoit Dupont, la cybersécurité est un élément important d'une politique gouvernementale suivant l'institution d'où elle émane, B. DUPONT, préc., note 42. Ainsi donc, les Etats-Unis qui publient leur cyberstratégie par le Chef de l'Etat accorde une plus grande importance à la cybersécurité que le ferait le Canada qui le publie par son ministère de la sécurité publique.

. Le CSTC

L'institution est à la fois « un service de renseignement électromagnétique (SIGINT)[253] à l'appui des politiques étrangères et de la défense, et un service de protection des renseignements et des communications électroniques […] » [254] . Il collecte les renseignements étrangers susceptibles d'aider le gouvernement fédéral à adopter des mesures de cybersécurité adéquates. Le Centre est régi par la *Loi sur la Défense nationale* qui, en son article 273.64 (1c), l'autorise à « fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère ». Le service peut également effectuer des collectes de renseignements sous la direction de son ministère de tutelle, le SP. Suivant la stratégie canadienne, le CSTC est :

> « reconnu à l'échelle internationale pour son expertise en matière de lutte contre les cybermenaces et les cyberattaques. Compte tenu de son mandat particulier et de ses connaissances sans pareil, le [CSTC] accroîtra sa capacité de détecter et découvrir les menaces, de fournir des services du renseignement étranger et de cybersécurité, et de faire face aux cybermenaces et cyberattaques contre les réseaux et systèmes de technologie de l'information du gouvernement. »[255]

Depuis 2011, le CSTC est très impliqué dans la protection et le renforcement des infrastructures critiques et, à cet effet, il a accompli plusieurs charges définies par la stratégie de cybersécurité[256]. Les plus importantes portent sur la création du Centre d'évaluations des cybermenaces (ci-après CECM). Son rôle principal est de détecter,

---

[253] L'acronyme est l'abréviation anglaise de Signals Intelligence. Selon le CSTC, le SIGINT s'entend du « renseignement électromagnétique […] [qui] désigne l'interception et l'analyse de communications et d'autres signaux électroniques. ». Voir en ligne https://www.cse-cst.gc.ca/fr/inside-interieur/signals-renseignement (consulté le 26 Novembre 2014).

[254] Pour plus d'informations, voir en ligne http://www.cse-cst.gc.ca/index-fra.html (consulté le 15 Juin 2014).

[255] Stratégie Canadienne, préc., note 1, p. 11.

[256] Par ailleurs, le projet de loi c-51 modifiant les pouvoirs d'enquête au 21ème siècle, actuellement en Chambre des Communes légalise des pouvoirs modernes d'enquête qui permettraient à la CSTC d'enjoindre des fournisseurs internet à fournir des données informatiques. Pour plus d'informations, voir *infra* note 281.

d'analyser et d'évaluer les menaces numériques[257]. Il détermine alors, à l'aide du Centre canadien de réponse aux incidents cybernétiques (ci-après CCRIC), des mesures préventives capables de juguler les risques de vulnérabilités au niveau des infrastructures du gouvernement canadien. Le CCRIC travaille également en coopération avec le Centre canadien du renseignement de sécurité (ci-après SCRS) pour lui indiquer des informations nécessaires à ses enquêtes. Dans l'optique d'amélioration des capacités du CCRIC, le CSTC a établi un programme d'échanges entre les employés du service et ceux du CSTC même. Le CSTC travaille en collaboration avec plusieurs autres organes fédéraux, afin de contribuer au renforcement de leurs capacités.

. Le SCRS

Au nombre des différents organes qui collaborent dans le processus de renforcement de la cybersécurité canadienne, le SCRS qui relève du SP tient sa compétence de la *Loi sur le service canadien du renseignement de sécurité*. L'organe surveille et met en œuvre des mesures de protection et pour neutraliser toute activité susceptible de nuire aux intérêts de l'État[258], que ce soit en dehors ou à l'intérieur de ses frontières géographiques[259], sous réserve de la satisfaction à certaines conditions préalables [260] indiquées par la loi. L'institution effectue des enquêtes sur les menaces qui planent et les risques éventuels découlant des vulnérabilités existantes, en recueillant des informations sur des individus suspects, des organisations ou autres entités étatiques ou non qui entrent dans son domaine d'investigation[261]. Suite à ces enquêtes, elle évalue les risques futurs et élabore

[257]CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS, *Centre d'évaluation des cybermenaces (CECM)*, disponible en ligne : https://www.cse-cst.gc.ca/fr/page/centre-devaluation-cybermenaces-cecm (consulté le 15 Septembre 2014).

[258] *LSCRS*, art 12.

[259]*Id*., art 16-1.

[260]*Id*.

[261] L'important pouvoir qui lui est conféré est parsemé de balises pour éviter les abus. Ainsi, la partie III de la *LSCRS* est exclusivement à la surveillance de cet organe de surveillance et la périodicité de ses rapports destinés au Ministère de la Sécurité publique limitent l'ampleur des surveillances que le service peut mettre en place, garantissant ainsi le respect de la vie privée des personnes et le respect des relations diplomatiques édictés par la *Loi constitutionnelle de 1982, Annexe B de la Loi de 1982 sur le Canada* (R-U), 1982, c 11.

des recommandations qu'elle intègre dans un rapport destiné au gouvernement qui sert aussi à le tenir informer de la tenue de ses activités et à « produire du renseignement »[262].

. La GRC

La cybersécurité est également une charge de la GRC suivant la *Loi sur la Gendarmerie Royale du Canada*[263]. Elle attribue à l'institution le rôle de déceler, prévenir et réprimer les infractions prévues au *Code criminel*[264] pouvant porter atteinte aux libertés civiles, aux biens publics ou encore à la sûreté gouvernementale. Elle joue également un rôle actif dans la collecte[265] et la communication des renseignements de sécurité et assure la circulation sécuritaire des communications qui s'établissent dans les domaines sensibles en collaboration avec le SCRS et le CSTC[266].

[262]L'organisme a également le mandat d'étudier les renseignements des futurs immigrants pour vérifier qu'il ne représente pas de risque sur le territoire. Il analyse aussi les demandes d'accès à des renseignements aux fins de conseiller le gouvernement sur la sensibilité de ces informations et les implications de ces divulgations.

La compétence du service s'étend également sur le réseau internet et, dans le champ de la cybersécurité canadienne, il est chargé des mêmes fonctions prévues par la LSCRS, étendues cette fois sur la toile . Il est donc laissé à son entière discrétion le déploiement de l'armada nécessaire pour prévenir les menaces technologiques, analyser les vulnérabilités existantes et recommander les mesures à prendre pour renforcer les systèmes, tout ceci dans une continuelle collaboration avec les organismes et ministères fédéraux et provinciaux. Le SCRS garantit la conservation des renseignements de sécurité, de quelque nature que ce soit et, dans une large mesure, pouvant être convoités par les puissances étrangères ou des terroristes. Sa large compétence et sa place dans la lutte contre les agressions cybernétiques prouvent la nécessité comprise de la lutte contre la prégnance des menaces d'envergures dans le fonctionnement étatique; voir Renforcer la résilience, préc., note 182, p. 37. La communication de ces renseignements est cependant restreinte dans la majeure partie aux seuls organes d'application de la loi intérieur ou internationaux sous couvert de l'autorisation préalable des autorités désignées, voir à cet effet, l'art 19 de la *LSCRS*, préc., note 211; SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ, préc., note 155, p. 32.

[263]*Loi sur la Gendarmerie royale du Canada*, LRC 1985, c R-10.

[264]*Code criminel*, préc., note 4.

[265]Dans son rôle de prévention, la GRC établit des « Programmes de sensibilisation » pour déceler et empêcher très rapidement les fiefs qui représenteraient une menace. Voir GOUVERNEMENT DU CANADA, préc., note 182, p. 18.

[266]La GRC dirige aussi des équipes spécialisées dans la collecte des renseignements de sécurité et de leur analyse, ce qui lui permet de procéder à des évaluations claires des menaces. Pour plus d'informations, lire généralement Renforcer la résilience, préc., note 182, p. 20.

Dépendamment de leur compétence, les organes ministériels et services affiliés opèrent une défense passive et/ou active[267]. Leurs relations sont fondées sur une hiérarchie ou une collaboration. Par ailleurs, ces institutions publient aussi des directives de cybersécurité à l'endroit des administrations publiques. Elles concourent dans le même temps à leur application.

B. Quelques mesures de défense passive et active

Le gouvernement du Canada a élaboré plusieurs stratégies technologiques de défense et de prévention cybersécuritaires en misant sur une veille numérique pour la contre-offensive et aussi sur la mise en place de logiciels de protection, de défense et de réponse en temps réel contre les MSP. Cette dynamique de cybersécurité passe aussi par la publication de directives de précaution à prendre en compte par les citoyens, les entreprises et à appliquer au sein des ministères[268] (défense passive). A ce jour, le gouvernement n'a pas publié d'informations précises sur la défense active qu'il a mise en place. Il est toutefois possible d'avoir accès à quelques mécanismes de gestion des cyberincidents.

. Un guide de pratiques exemplaires dans les ministères et autres organes étatiques affiliés

Les cyberintrusions ciblées, signe indicatif d'une MSP[269], visent les points névralgiques des structures virtuelles exploitées par les membres d'un gouvernement. A ce titre, ce sont les structures gouvernementales vitales au fonctionnement de l'État qui seront visés[270].

[267] Les cyberdéfenses passive et active sont des notions avancées par James LEWIS pour décrire d'une part l'ensemble des mesures gouvernementales mises en place par le gouvernement pour prévenir les cyberattaques (passive) d'une part, et pour répondre en temps réel en cas de cyberattaques (active) d'autre part. J. LEWIS, préc., note 14, p. 66.

[268] Protéger une société ouverte, préc., note 244, p. 11- 12.

Pour colliger ces risques de piratage, le CSTC a élaboré, pour chacune des étapes de connexion ou de traitement numérique, des recommandations de protection indispensable à l'utilisation exemplaire de l'informatique afin de garantir une tranquillité des employés des ministères, d'une part et des usagers du service public, d'autre part.

Au sein des ministères et autres organes affiliés de l'État, des solutions d'atténuations de risque de cyberintrusions ciblées ont été élaborés par le CSTC. La plus récente publication non classifiée en ce sens date de Novembre 2014 et comporte des mesures de prévention à mettre en place par le gouvernement. Suivant l'organisme de sécurité, « la mise en œuvre des 10 mesures d'atténuation les plus efficaces empêchera la grande majorité des cybermenaces actuellement détectées sur les réseaux du [gouvernement du Canada] ». Ces mesures touchent entre autres aspects du réseau, l'accès des applications en encourageant la création d'une liste blanche. Cette liste, appelée liste blanche des applications[271], sert à contrôler toutes les applications qui accèdent au réseau en procédant par nom de fichier, par taille ou encore par type de fichier[272]. Suivant le tableau élaboré par le CSTC, les ministères devraient mettre en place un système de gestion des correctifs pour les applications qui n'ont pas encore eu de mise à jour et donc comporte des «risques

[269] SÉCURITÉ PUBLIQUE CANADA, *Principes de prévention contre les menaces sophistiquées et persistantes, Numéro*, TR11-002, 02 Décembre 2011, disponible en ligne https://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-002-fra.aspx (consulté le 2 Novembre 2014).

[270] *Id.*

[271] CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS, *Utilisation d'une liste blanche des applications - Conseils à l'intention du gouvernement du Canada*, ITSB-95, Janvier 2013, disponible en ligne : https://www.cse-cst.gc.ca/fr/node/242/html/9857 (consulté le 20 Novembre 2014). Cette liste est le fruit de la combinaison d' « un produit logiciel permettant de sélectionner et d'approuver les exécutables et bibliothèques de logiciels nécessaires », et « des listes de contrôle d'accès permettant d'empêcher les utilisateurs de modifier les fichiers approuvés ». La liste blanche de contrôle des applications est « conçue spécifiquement pour empêcher l'exécution de programmes malveillants et non autorisés. Elle permet de s'assurer que seuls les programmes (fichiers exécutables ou EXE) et les bibliothèques de logiciels (DLL) spécifiquement sélectionnés peuvent être lancés, ce qui bloque l'exécution de tous les autres programmes et bibliothèques». Elle est mise en œuvre suivant des étapes précises qui vont de l' « [identification] des exécutables et bibliothèques de logiciels dont l'exécution doit être permise sur un système donné », du blocage de « l'exécution de tout autre exécutable ou bibliothèque de logiciels sur ce système » à la limitation des accès à la modification de la liste.

[272] CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada Bulletin de sécurité des TI à l'intention du gouvernement du Canada*, ITSB-89 Version 3, Novembre 2014, disponible en ligne : https://www.cse-cst.gc.ca/fr/node/1304/html/24334 (consulté le 2 Décembre 2014).

d'exploitation » de vulnérabilités qui y sont contenues. Une précaution similaire porte sur le renforcement des systèmes d'exploitation (SE) opéré selon la structure numérique adoptée par chaque organisme. Sachant qu'au sein de plusieurs ministères canadiens, jusqu'en 2014, c'est le SE Windows 7 Entreprise[273] qui était utilisé; le CSTC a publié des recommandations visant à en renforcer la configuration[274].

Les insuffisances de ces guides portent essentiellement sur le dépassement de ces mesures de précautions par les avancées technologiques, mais aussi par le nombre important d'usagers des services administratifs étatiques. Prenons le cas des mesures purement technologiques adoptées par la hiérarchie au sein d'un ministère telle que la liste des applications. Elle est intéressante en ce qu'elle limite l'accès à certaines applications qui pourraient être nuisibles, qui sont peut être connues et répertoriées par les SE. Cependant, elle ne bloque pas les nouvelles applications qui pourraient être développées par les pirates informatiques[275]. Les précautions prises à l'endroit des usagers à l'échelon inférieur comme la dispense de cours ont un degré d'effectivité faible en ce sens qu'elles sont limitées par l'application réelle qu'en feront les usagers. En dépit du fait que la personne humaine soit au centre de toutes les utilisations qui se font de l'informatique et en demeure donc la principale porte d'entrée, les mesures techniques directes semblent donc être plus appropriées au problème.

. La gestion des cyberincidents

Dans le cadre de la défense active, l'autorité étatique a élaboré plusieurs corps de règles destinées au public ayant pour but de permettre une gestion rapide des cas de cyberincidents décelés ou déclarés.

---

[273] *Id*., p. 2; CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS, *Conseils en matière de configuration de renforcement de Microsoft Windows 7 Entreprise*, ITSB-110, Octobre 2014, disponible en ligne : https://www.cse-cst.gc.ca/fr/node/1298/html/24269(consulté le 20 Décembre 2014).

[274] CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS, préc., note 272.

[275] Bruce SCHNEIER, *Schneier on security*, 1st ed., New York, Wiley publishing, 2008, p. 227.

En ce sens, le Conseil du trésor canadien a publié un cadre de gestion des incidents cybernétiques[276] dont le mode d'encadrement varie selon le degré de gravité de l'attaque contre les structures gouvernementales virtuelles. On y note que les attaques cybernétiques qui causent des pertes en vies humaines comportent un degré très élevé de dangerosité pour la stabilité sociale et l'économie canadienne[277]. Suivant le tableau élaboré par le CCRIC, les réponses à ces cyberattaques doivent être coordonnées au niveau des organes d'urgence existant au niveau de chaque structure étatique. Ces réponses sont également empreintes du secret d'État concernant la situation exacte des dégâts et/ou des causes réelles de ces dégâts[278]. La réaction d'urgence à une attaque cybernétique est, par ailleurs, prévue au niveau de chaque « gouvernement fédéral, provincial et territorial »[279] et est coordonnée par le Système national d'intervention d'urgence (SNIU). Il revient à cette dernière d'« incorpore[r] et [opérationnaliser] les principes de gestion des urgences établies dans le [cadre de sécurité civile pour le Canada (CSCC)] ».

En définitive, dans ses publications, le gouvernement ne mentionne pas ses capacités technologiques réelles de contre-offensive, ce qui limite l'information portée au public aux grandes lignes de la défense passive; la sécurité intérieure justifiant probablement ce silence[280]. De plus, il n'existe pas dans l'ordonnancement canadien des types d'infractions constituées comme telles dans le cyberespace de façon spécifique.

---

[276]SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Plan de gestion des incidents de la TI du gouvernement du Canada », en ligne http://www.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimtipr-fra.asp (consulté le 14 Décembre 2014). Ce document non classifié expose les différentes étapes d'une défense active en cas de cyberattaques.

[277]*Id.*

[278]*Id.*

[279] La gestion des situations d'urgence est contenue dans la *Loi sur la gestion des urgences* L.C. 2007, ch. 15 sur laquelle le gouvernement s'est basé pour élaborer le procédurier d'urgence en cas de cyberincidents des technologies de l'information : Secrétariat du Conseil du Trésor, préc., note 276.

[280]Contrairement au Canada, les États-Unis publient d'intéressantes informations sur leur défense active. Voir par exemple Robert RADVANOVSKY et Allan MCDOUGALL, préc., note 38, p. 51-73.

La cybercriminalité demeure un enjeu majeur du siècle actuel et la volonté de l'enrayer ressort des textes de loi proposés par le gouvernement depuis 2010[281]. Cet impératif[282] concerne toutes les institutions gouvernementales d'où leur totale implication dans la stratégie de lutte contre le cybercrime. L'absence d'adoption de ces projets de lois entraînerait une ratification tardive de la Convention de Budapest, créant un écart entre les partenaires du Canada et celui-ci. En effet, lorsque l'analyse porte sur la place de la cyberstratégie canadienne dans sa politique de défense, il est aisé de constater qu'elle se

[281]Le projet de loi C-12 vise à donner plus d'outils facilitant les enquêtes par les institutions d'application de la loi et à apporter des éclaircissements terminologiques. Le projet de loi c-13 portant modification du Code Criminel, du droit de la preuve et de l'entraide judiciaire a été introduit au Parlement par le Ministère de la Justice. Il est intéressant en ce qu'il aborde « les violations commises à l'aide de tous moyens de communications ». Ensuite, le projet de loi C-47 qui porte le pouvoir de mise en demeure de produire adressé aux fournisseurs d'accès et de services. Ce projet oblige les télécommunicateurs à fournir des informations afin de faciliter les enquêtes telles l'obligation de développer des moyens techniques d'interception et de transmission des données collectées. Un autre projet de loi, le C-51 vient ajouter au Code Criminel, l'infraction lié à l'importation, l'utilisation et la mise à disposition des virus informatiques avec l'intention de commettre un forfait. Enfin, le projet de loi c-52 vient encadrer les procédures d'enquêtes liées à l'accès aux renseignements des individus par les autorités compétentes d'enquêtes et de contrôle du respect de l'application de la loi. Il institue l'interception des communications en temps réel, l'accès légal et la saisie de données. Pour plus d'informations, voir les résumés législatifs de ces projets : PARLEMEN DU CANADA, Division des affaires juridiques et législatives, *Résumé législatif du projet de loi C-12 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques*, 19 octobre 2011, disponible en ligne : http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=C12&Mode=1&Parl=41&Ses=1&source=library_prb&Language=F (consulté le 17 Août 2014); PARLEMENT DU CANADA, Division des affaires juridiques et législatives, *Résumé législatif du projet de loi C-13 : Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle*, Julia NICOL et Dominique VALIQUET, 11 Décembre 2013, (révisée le 28 Août 2014), disponible en ligne :http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=F&Mode=1&DocId=6731159&File=4(consulté le 6 Septembre 2014); PARLEMENT du CANADA, Division des affaires juridiques et législatives, *Résumé législatif du projet de loi C-47 : Loi sur l'assistance au contrôle d'application des lois au 21e siècle*, n° LS-655F, Dominique VALIQUET, 28 Juillet 2009, disponible en ligne http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=C47&Mode=1&Parl=40&Ses=2&source=library_prb&Language=F#ftn8 (consulté le 17 Octobre 2014); PARLEMENT du CANADA, Division des affaires juridiques et législatives, *Résumé législatif du projet de loi C-51 : Loi sur les pouvoirs d'enquête au 21e siècle*, n° 40-3-C51F, Dominique VALIQUET et Katherine SIMONDS, 3 Février 2011, disponible en ligne : http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?Language=F&Parl=40&Ses=3&Mode=1&ls=C51&source=library_prb#a2 (consulté le 17 Octobre 2014); PARLEMENT DU CANADA, Division des affaires juridiques et législatives, *Résumé législatif du projet de loi C-52 : Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention*, Erin SHAW et Dominique VALIQUET, 30 mai 2011, disponible en ligne : http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?Language=F&ls=c52&Parl=40&Ses=3&source=library_prb (consulté le 10 Octobre 2014).

[282]D. VALIQUET et H. PORTEOUS, préc., note 137.

situe dans une faible moyenne[283] de réelle dynamique de lutte contre le cybercrime majeure[284].

La préoccupation gouvernementale de l'avancée des crimes majeurs l'a amené à considérer la puissance des alliances entre États et son implication dans les activités mondiales de lutte. Cela constitue un aspect majeur de sa stratégie de renforcement de ses capacités nationales de lutte contre le terrorisme[285] puisqu'il révèle la nécessité de s'allier à des institutions internationales et interétatiques spécialisées[286] et d'intervenir davantage dans les fora internationaux[287]. À cet effet, le gouvernement a noué plusieurs alliances régionales et internationales qui peuvent servir à ce renforcement.

Section 2 : Les apports des mécanismes régionaux et internationaux de cybersécurité

Au su de la vitalité des infrastructures critiques numériques et gouvernementales que nous évoquions plus haut et du risque encouru en cas de cyberattaque, plusieurs autorités étatiques ont établi des alliances afin d'unifier leurs efforts pour améliorer leur résilience. Le Canada intervient en ce sens dans son partenariat avec les États-Unis duquel est ressorti le Plan d'action *Par-delà les frontières* (ci-après Plan d'action)[288] (Paragraphe 1) et, d'autre part, au sein du cadre multilatéral Five Eyes (ci-après FVEY) auxquels sont partis l'Australie, la Nouvelle-Zélande, l'Angleterre, le Canada et les États-Unis

[283] B. DUPONT, préc., note 42, p. 73. Selon l'auteur, cette moyenne est davantage perçue lorsqu'on considère le coût du budget, l'origine institutionnelle et le choix du type de mesure adopté.

[284] Rafal Rohozinski, leader du groupe canadien de cybersécurité SecDev affirme lui : « Canada has interesting expertise but those capabilities are not reflected in government, […] ». SDA, préc., note 9, p. 54.

[285] Renforcer la résilience, préc., note 182, p. 14.

[286] *Id.*

[287] *Id.*, Protéger une société ouverte, préc., note 244, p. 8 et 10.

[288] Soucieux de la sécurité de leurs frontières, les États-Unis et le Canada ont choisi de travailler ensemble sur le long terme : « Cette déclaration établissait un nouveau partenariat à long terme qui s'articule autour d'une approche de la sécurité et de la compétitivité économique qui repose sur le périmètre commun ». Voir : GOUVERNEMENT DU CANADA, *Par-delà la frontière : une vision commune de la sécurité du périmètre et de la compétitivité économique*, 2011, disponible en ligne http://plandaction.gc.ca/fr/content/dela-la-frontiere (consulté le 8 Août 2014) [Plan d'action].

(Paragraphe 2). Nous étudierons donc dans cette section, les aspects couverts par les ententes qui émerge de ces collaborations interétatiques.

Paragraphe 1 : La résilience *Par-delà les frontières*

Les rapports de sécurité liant le Canada et les États-Unis se sont intensifiés suite au bug de l'an 2000[289]. Ce partenariat entre les deux gouvernements a donné lieu à la signature de plusieurs ententes portant pour la plupart sur le renforcement des actifs communs et la protection au niveau des frontières partagées. Le Plan d'action, publié en 2011, fait état de différentes mesures visant l'amélioration de la cybersécurité en définissant les grandes lignes d'une coopération à l'international (A). Ce plan aborde cependant de façon imprécise les voies à suivre pour la mise en place d'une cybersécurité efficace. Il importe à cet effet de penser à des pistes d'amélioration de cette collaboration bilatérale (B).

A. La volonté commune de coopération internationale

Le plan cherche à créer un leadership commun au sein des instances internationales et encourage l'implication dans les coopérations avec les États-tiers [290]. Les deux gouvernements visent ainsi le « leadership conjoint dans la participation aux démarches internationales touchant la cybersécurité »[291]. De fait, les objectifs canadiens et américains seraient mis de l'avant dans les dynamiques internationales afin d'être pris en compte lors de l'adoption de dispositions relatives à une cybersécurité globale. Dans cette logique, le texte mentionne spécifiquement la nécessité pour le Canada de ratifier la Convention : «

[289] W. de LAAT, préc., note 53, p. 2. L'auteur précise toujours à la même page: : « In a Canada-United States context, these networks and systems-be they computer networks, electric power grids, pipelines, transportation and logistics networks, or supply chains--together form the essential underpinnings of an immense and highly prosperous North American economy. »

[290] Au sens du Plan d'action, les États tiers sont entendus comme les pays ne faisant pas partie du partenariat.

[291] Plan d'action, préc., note 288, p. 32.

[…] le Canada accédera à la Convention sur la cybercriminalité du Conseil de l'Europe, et nos deux pays examineront également les possibilités de promouvoir cette convention »[292].

Outre cette volonté commune de participer activement à la réflexion internationale d'une cybersécurité efficace, le Plan d'action propose également d'autres initiatives, à savoir : la réalisation des programmes et le développement de produits pour augmenter la sécurité des infrastructures essentielles, la création de mécanismes d'évaluation des risques, et l'amélioration de la coopération dans le cadre du renforcement des infrastructures numériques et « augmenter la capacité des pays à faire face conjointement aux MSP ».

Au su de la dangerosité des MSP et de l'incidence qu'elles peuvent avoir sur la société canadienne, des mesures sérieuses, précises et concrètes devraient être prises par les protagonistes de l'entente sur son amélioration de part et d'autre de la frontière commune. Le Plan d'action ne fait mention que de deux mesures très vagues à adopter par l'une ou l'autre des parties, soit : « Accentuer le leadership conjoint dans la participation aux démarches internationales touchant la cybersécurité » et « Protéger les infrastructures gouvernementales et numériques essentielles d'importance binationale et accroître le caractère sécuritaire du cyberespace pour tous nos citoyens »[293]. À l'étude de ces mentions du Plan d'action, il apparaît que la cybersécurité semble une problématique sous-abordée. Cela est-il fait à dessein?

Ne pouvant concrètement répondre à cette question, nous nous contenterons d'élaborer des pistes de réajustement essentielles qui doivent être pris en compte dans ce partenariat entre les deux puissances.

---

[292] *Id*.

[293] Pour chacun de ses points, les mesures des progrès effectués sont vaguement définies. On peut lire pour l'objectif de protection des infrastructures gouvernementales, aucune précision claire n'est donnée :

> « Sécurité publique Canada, le département d'État des États-Unis et le département de la Sécurité intérieure des États-Unis feront rapport des engagements conjoints ou coordonnés avec le secteur privé et d'autres intervenants externes, faisant état notamment des séances d'information et exposés conjoints, de l'assistance fournie dans le contexte d'un incident dans le cyberespace et des produits conjoints de communication qui auront été mis au point. »

V. Plan d'action, préc., note 285, p. 31

B. Les pistes d'amélioration de la coopération pour une cybersécurité effective

W. de Laat écrit:

> « In order to sustain joint efforts, Canada and the United States must immediately develop an ambitious, comprehensive, binational plan, setting out in detail how the two nations will work together to prepare for, respond to, and recover from cyber and critical infrastructure threats and disruptions. »[294]

En effet, définir des grands axes d'un plan d'action sur la cybersécurité ne devrait pas se limiter aux différents aspects énoncés plus haut. Aujourd'hui, la cybersécurité est un élément incontournable de toute activité commerciale, économique et sécuritaire, cela explique donc qu'il ait été intégré à l'ensemble du Plan. Toutefois, au su des enjeux en présence, de la vitalité des infrastructures interdépendantes et interconnectées, les axes définis devraient comporter de précisions et constitué un cadre complet et précis indicatif des efforts à déployer.

Selon Rosenzweig, lorsque deux États partagent autant d'infrastructures communes, « seulement un solide plan conjoint de système de défense a une chance de succès »[295]. Lui faisant écho, Michael McDaniel écrit que la coopération bilatérale serait complète si elle incluait « information sharing, standard cross border assessment risk, planning, emergency assistance and emergency planning, and the formal establishment of sustainable consortia »[296].

Dans cette même logique, nous estimons qu'au vu des enjeux qui ressortent de l'exploitation du cyberespace, la cybersécurité devrait faire l'objet d'un plan d'action intégral comportant les spécificités propres aux interconnexions des infrastructures

---

[294] W. de LAAT, préc., note 53, p. 6.

[295] Emmanuel BRUNET-JAILLY, « The New Perimeter Initiative: Will Security Trump Trade? », **(**Fall 2012**)**, 37 *Can.-U.S. L.J.* 273 1, 7.

[296] *Id*.

communes. Ce plan devrait comporter un volet sur les rôles de chaque ministère et de ses sous-organes et rappeler les dispositions prises pour la gestion des cyberincidents[297]. Pour de Laat, un plan de cette nature devrait inclure « à la fois une sécurisation du cyberespace et un volet sur les infrastructures communes qui dépendent de cet environnement »[298]. Concernant ces infrastructures, il conviendrait que soit mis en place un tronc commun de ressources et de moyens institutionnels réactifs permettant de répondre en temps réel à un cyberincident[299]. A cet effet, les partenaires devraient publier des guides de bonnes habitudes sécuritaires et planifier des séances de simulation de cyberincidents[300]. Le plan devrait également convenir de séances de concertation périodiques avec les experts du secteur privé afin de relever les différents défis cybersécuritaire auxquels ils sont confrontés et les solutions qui peuvent y être apportées pour retrouver rapidement toutes leurs capacités[301]. Cette proposition est d'autant plus pertinente que les infrastructures essentielles sont composées de plusieurs entreprises privées qui sont partenaires avec le secteur public. Il importe à cet égard que le potentiel plan d'action pour le cyberespace, comme nous le recommandons ici, le mentionne clairement[302].

Par ailleurs, nous l'avons noté, le texte fait seulement état de la ratification de la Convention européenne sans mettre l'accent sur la nécessité de créer des cadres internationaux de travail destinés à établir des ententes internationales qui aurait vocation

[297] William de Laat explique par exemple que les Etats doivent élaborer un plan précis de partenariat portant exclusivement sur la cybersécurité. W. de LAAT, préc., note 53, p. 6.

[298] *Id*.

[299] *Id*. [note 72]. Certes, il existe déjà un cadre commun de gestion des cyberincidents mais celui-ci semble rencontrer des difficultés.

[300] *Id*.

[301] *Id*., p. 6-7. L'auteur s'interroge à savoir si les deux puissances ne devraient pas consacrer plus d'efforts à une défense active plutôt que passive. Il écrit ceci: « But are the two nations still placing too much emphasis on threats and vulnerabilities and not enough on how we deal with the actual consequences of a major failure or attack? What specific activities do they have in mind for developing more resilient joint response and recovery capabilities? »

[302] W. de LAAT, préc., note 53, p. 7.

à s'appliquer aux MSP. Il ne précise pas non plus les tenants de telles coopérations ou simplement les instances internationales avec lesquels ils envisagent de coopérer[303].

A l'instar de la coopération bilatérale qui lie les deux puissances, une autre alliance impliquant d'autres pays renforce leurs intérêts communs. Cette alliance des différents services de renseignement des FVEY[304] peut également concourir à lutter contre les MSP.

Paragraphe 2 : La contribution de l'alliance des FVEY

Les FVEY visent principalement la collecte et l'échange d'informations de sécurité. Puisque cette coopération multilatérale est fondée sur l'échange d'informations sensibles[305], toutes les activités concrètes et leurs avancements ne sont pas accessibles au public. Il importe de mentionner que ces agences ne travaillent pas systématiquement ensemble. Elles interviennent de concert lorsqu'il s'agit d'élaborer des axes de défense communs. Il semble évident que ces échanges informationnels soient de nature à concourir à une lutte efficace contre le cyberterrorisme (A). Toutefois, cette affirmation ne tient pas pour le cyberespionnage étatique (B).

A. L'apport de la surveillance des FVEY contre le cyberterrorisme ?

Tous les individus produisent des signaux qui permettent de tracer leurs activités, leurs habitudes, de déceler la préparation d'un projet terroriste ou pas.

Nous l'avons vu, les cyberterroristes utilisent beaucoup l'internet comme outil de communication, de propagande, de planification, de recrutement, etc. Ils fournissent alors

[303] *Id*.

[304] Pour des informations sur le cycle de traitement des informations au sein des agences de remseignement, il est intéressant de consulter : Dr Colin ROGERS, « Intelligence gathering and police systems » dans Imran AWAN et Brian BLACKEMORE, préc., note 75, p. 127-141.

[305] Par information sensible, nous entendons par exemple, les dernières améliorations de défense militaire.

des données utilisables. Dépendamment de la collecte qu'opéreront les agences, ces données peuvent être liées au trafic[306] (appelés métadonnées) ou au contenu[307]. Ce sont ces informations ou indices qui permettraient de démanteler une organisation terroriste. Cependant est-ce que cette surveillance pourrait être utile dans les enquêtes sur les cyberterroristes agissant seuls (communément connus sous l'appelation « loup solitaire)[308]?

Si l'on considère que ce sont des personnes très ordinaires, c'est-à-dire menant un train de vie « normal », avec une existence sur les réseaux sociaux communs sans revendication idéologique ou religieuse affichée, il est difficile d'imaginer que des données collectées puissent servir. A moins que ces communications ne portent sur la préparation de l'acte, la difficulté demeure. En effet, les loups solitaires auraient tendance à agir dans la plus grande discrétion et, donc, de se fondre dans la masse au quotidien[309].

Les récentes attaques terroristes ont conduit à pousser plus loin la surveillance électronique par la mise au point d'un algorithme capable de déceler des activités des internautes des traits assimilables à un terroriste ou à une personne susceptible de se radicaliser. Cet algorithme fonctionnerait donc sur la base des cas antérieurs enregistrés. Ces cas serviraient alors de modèle de reconnaissance d'un cyberterroriste. B. Dupont doute de l'efficacité de ce qu'il décrit comme étant du « solutionnisme »[310]. Il l'affirme, à bon escient :

---

[306] Voir *infra*, p. 101 ; note 457 et 458.

[307] *Id*.

[308] Benoît DUPONT, « Pourquoi les mégadonnées et la surveillance généralisée ne nous protègeront pas contre le terrorisme », 28 Mars 2015, disponible en ligne http://www.benoitdupont.net/node/179 (consulté le 2 Avril 2015).

[309] C.P. DAVID et B. GAGNON, préc., note 57, p. 244.

[310] Benoit DUPONT, « Pourquoi les mégadonnées et la surveillance généralisée ne nous protègeront pas contre le terrorisme », préc., note 303. Citant Evgeny MOROZOV dans son article, Benoît Dupont décrit cette tendance qui voudrait que l'internet en général et es réseaux sociaux en particulier soient mieux surveillés. Il écrit à ce propos :

> « S'il n'a pas semblé très difficile à ceux que l'on désigne comme des « loups solitaires » d'échapper à la vigilance des services anti-terroristes, le raisonnement

> « […] [L]es corrélations qui permettent de prédire certains comportements ne sont significatives et fiables que lorsque ceux-ci peuvent être observés de manière suffisamment fréquente. Or, si cela ne pose pas de problème pour les habitudes de consommation quotidiennes de milliards d'usagers, il se trouve bien heureusement que les attentats terroristes commis par des individus isolés restent des événements exceptionnels, et donc impossibles à modéliser. Bien que les forums extrémistes regorgent de participants tenant des propos faisant l'apologie de la violence, seule une infime minorité d'entre eux passe des paroles aux actes et représente une menace sérieuse méritant une prise en charge par les services de renseignement. La NSA, avec ses ressources technologiques quasiment illimitées et ses bataillons de mathématiciens aurait certainement éradiqué le phénomène si un algorithme miraculeux permettait d'identifier avec certitude le prochain « loup solitaire » à partir d'élucubrations contenues dans un profil Facebook »[311].

À défaut de pouvoir analyser une méthode connue des renseignements de sécurité, nous nous bornerons à cet exemple. Cette tendance pouvant être sérieusement envisagée par l'une des agences de renseignements des FVEY, il est intéressant de voir que le partage des SIGNIT et l'augmentation des surveillances électroniques ne sont pas une panacée pour le problème du cyberterrorisme. À l'instar de son implication sur la vie privée des individus[312], ce procédé conduirait à d'innombrables pistes qui seraient pour la plupart non concluantes. Elle apporterait des éléments de solutions mais ne permettrait pas de traquer et de mettre la main sur tous les cyberterroristes.

Pour ce qui est du cyberterrorisme parrainé par les États, les difficultés demeurent, mais à cela s'ajoute celle du secret des activités des services de renseignements. Même si

---

> proposé par ceux qui réclament une surveillance systématique de l'Internet en général, et des plateformes de médias sociaux en particulier, est que nous devrions plutôt songer à confier la tâche d'identifier les profils suspects d'individus « auto-radicalisés » à des outils informatiques omniscients. Alimentés par les milliards de données publiées quotidiennement par les usagers – y compris ceux qui professent les idées les plus violentes – sur leurs profils personnels ou les forums de discussion, et par les métadonnées produites par leurs activités en ligne, ces outils permettraient alors à des algorithmes de détecter de manière automatisée la menace terroriste avant qu'elle ne se concrétise, en identifiant notamment les mots-clés ou les sentiments extrêmes laissant envisager un passage à l'acte imminent. »

[311] *Id.*

[312] CHAMBRE DES COMMUNES DU CANADA, Comité permanent sur la défense nationale, Témoignage de Rafal Rohozinski, NDDN, n° 38, 2ème session, 41ème législature, 20 Novembre 2014, p. 7.

l'activité de cyberterrorisme était décelée, il serait surprenant que l'implication d'un allié soit dénoncée par un autre État des FVEY.

Qu'en est-il du cyberespionnage étatique?

B. Pourquoi les FVEY ne sont-ils pas utiles dans la lutte contre le cyberespionnage étatique?

L'étude de l'effectivité des mesures adoptées par les services de renseignements pour une régulation du cyberespionnage étatique est impossible. La raison étant toute simple, ce sont les agences de renseignements qui mettent en place les dispositifs de surveillance des autres agences et de leur gouvernement. C'est ce que nous a appris le programme *Prism*[313].

La révélation de *Prism* aura globalement permis de dévoiler une collecte massive de métadonnées, extraites des téléphones mobiles, des ordinateurs et des comptes de personnalités politiques. Le programme impliquait des membres des FVEY avec à la tête la *National Security Agency* (ci-après NSA) des Etats-Unis.

[313] Pour plus d'informations, voir Mickael DORIGNY, « Le projet NSA-Observer » 28 Juillet 2014, disponible en ligne : http://www.information-security.fr/projet-nsa-observer/ (consulté le 2 Avril 2015). On peut y lire que le programme fait partie d'un ensemble de manœuvres d'espionnage effectuée par les Five Eyes. Mickael DORIGNY décrit les trois composantes de ce système :

> « Upstream : Il s'agit d'un programme visant principalement l'écoute systématique et l'enregistrement des communications passant par les câbles de fibre optique transatlantiques. On parle alors de collecte massive d'information comme les metadata, les données dites « internet », les fax ou données téléphoniques… Les projets TAMPORA et RAMPART(-A) sont les équivalents de ce programme pour le GCHQ et les autres pays des Five-Eyes.
> PRISM : Le programme PRISM est celui qui a eu le plus de retentissement médiatique aujourd'hui, il s'agit en faite d'une partie de l'ensemble des programmes et actions de l'agence de renseignement américaine. PRISM est l'équivalent de l'écoute massive Upstream sauf que les écoutes sont ici effectuées en accord avec les fournisseurs de services ou les hébergeurs de contenu, on peut par exemple citer Facebook, Yahoo! ou Google.
> Muscular : Muscular est un programme visant le vol des données au sein des grands hébergeurs de contenu mais cette fois-ci sans leur accords ».

Il serait aisé de déduire, au su du fort partenariat entre les pays alliés que le cyberespionnage ne concernerait pas leurs citoyens, voire leur gouvernement mais les révélations de Snowden nous auront démontré le contraire. En effet, la collaboration qui portait originellement sur la surveillance d'autres pays excluant donc les citoyens des membres-alliés a été subtilement détournée par les États-Unis qui ont collectés les métadonnées des citoyens de l'alliance[314].

Cette difficulté d'accès aux activités des services de renseignement ne se limite pas seulement à celle de cyberespionnage étatique. Elle les affecte toutes puisque ces agences et leurs organes affiliés produisent continuellement du renseignement de sécurité. Un peu plus haut[315], la notion du renseignement de sécurité avait été abordée et nous avions constaté sa vitalité et son importance dans les rouages de fonctionnement d'un gouvernement, en l'occurrence, canadien. A ce titre, puisque les FVEY sont composés exclusivement d'agences de renseignement, il ne peut être question d'estimer l'évolution et les conséquences de leurs activités sur la lutte d'une MSP comme le cyberespionnage étatique dont il est question.

Cette constatation ne sous-entend cependant pas qu'il est impossible d'élaborer des voies communes de régulation internationale contre ces menaces. L'adoption majoritaire d'un code de bonne conduite apparaît encore plus urgent et d'actualité.

Nous sommes d'avis que l'engagement du SP à ratifier la Convention de Budapest[316] permettra au Canada de pouvoir identifier pénalement les MSP[317] afin de les combattre adéquatement[318]. Toutefois, comme mentionné plus haut, l'analyse du *jus ad bellum* nous

[314] James BALL, « US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data » 20 Novembre 2013, disponible en ligne : http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data (consulté le 18 décembre 2014).

[315] *Supra*, p. 47.

[316] Stratégie canadienne, préc., note 1, p. 8.

[317] D. VALIQUET et H. PORTEOUS, préc., note 137.

[318] La nécessité de comprendre la définition et de connaître la qualification des cybercrimes majeurs ou MSP est une condition sine qua none d'une bonne défense active.

permettra d'identifier la qualification de ces activités au niveau de la communauté internationale dans le cadre notamment du cyberespionnage étatique et du cyberterrorisme parrainé par les États. L'étude de l'étendue du texte conventionnel permettra aussi d'apprécier son apport à la protection des infrastructures canadiennes et de faire ressortir les obligations internationales qui incomberont au pays. Par ailleurs, la Convention ayant une vocation exclusivement pénale, il sera intéressant de considérer les indicatifs qu'il apporte dans l'imputabilité des actes aux auteurs étatiques.

TITRE II : L'application des dispositions internationales de lutte contre les MSP

Nous l'avons vu, les cyberattaques se déroulent dans le cyberespace où n'intervient pas la notion de frontières et introduit donc une nouvelle perception de la notion d'espace. Elles font intervenir des actes se déroulant dans un espace dématérialisé qui, dans la continuité de l'absence de frontières, n'est assujetti à aucun ordre étatique. Cette ubiquité et les néologismes qu'apportent l'Internet est propice à l'émergence de nouvelles formes d'actes considérés comme des crimes transnationaux. La position de la communauté internationale à cet égard semble ferme. Pour l'illustrer, certains textes issus d'ententes internationales, produit de diverses coopérations interétatiques bilatérales ou multilatérales pointent le cyberterrorisme et le cyberespionnage étatique comme des MSP[319]. L'autorité canadienne suit la même tendance, manifestant par le biais de son SP, son intention de freiner au mieux les assauts contre ses infrastructures critiques.

Force est toutefois de constater le vide juridique qui prévaut au plan international. En effet, pour contrer cette situation, il n'existe ni convention, ni traité international pointant spécifiquement ces actes. Quelles sont les causes de ce silence?

Ne pouvant certainement pas nous étendre plus qu'il n'en faut sur cette interrogation, notre étude se consacrera plutôt à l'analyse des textes existants, soumettant les relations interétatiques, pour faire ressortir les dispositions utiles à une lutte concertée contre le cyberterrorisme et le cyberespionnage étatique.

Le chapitre 1 du titre 1 de ce mémoire nous aura permis de sortir des traits communs aux deux notions. Il s'agit d'actes impliquant nécessairement l'usage d'un outil informatique, de l'internet et de maliciels et qui ont pour objectif de causer une difficulté à un État et, par-là, représentent un danger pour la personne humaine.

[319] Voir les textes issues des diverses coopérations qu'entretient le gouvernement canadien *supra*, note 44.

Ces liens communs nous ont permis de recenser des textes internationaux susceptibles de s'appliquer à ces problématiques. En ce sens, nous avons en premier lieu considérer les principes classiques des relations entre États afin d'évaluer la qualification juridique à donner aux cyberattaques. Ces principes ayant été adoptés bien avant l'avènement de l'internet[320], il apparaît utile d'explorer, en parallèle, d'autres textes internationaux pointant des crimes informatiques plus ou moins en lien avec la problématique sujet de notre travail.

Ainsi, dans ce titre second, nous aborderons la notion de bonne foi dans les relations interétatiques et appliquerons la qualification d'acte d'agression aux cyberattaques étatiques (Chapitre 1). Ensuite, la Convention de Budapest étant un texte moderne issu d'une coopération multilatérale contenant plusieurs ratifications à l'heure actuelle[321], nous analyserons son apport à notre étude, notamment en ce qui concerne le second volet essentiel à une législation internationale, la coopération internationale (Chapitre 2).

Chapitre 1 : Les principes internationaux post-guerres mondiales

Les relations internationales sont soumises aux grands principes coutumiers. Lorsqu'une violation d'une obligation survient, et entraîne des conséquences comme celles des cyberattaques d'origine étatique, c'est le *jus ad bellum*[322] qui s'applique[323]. Pour qu'une

[320] Matthew E. CASTEL, « International and Canadian Law Rules Applicable to Cyber Attacks by State and Non-State Actors » **(**Juin 2012**)** 10 Can. J. L. & Tech. 89 6.

[321]Elle regroupe plus de 55signatures dont celles de six pays non européens. Pour plus d'informations sur la liste des pays signataires, voir CONSEIL DE L'EUROPE, Bureau des Traités, Convention sur la cybercriminalité, 23 Novembre 2001, STE n°185, disponible en ligne http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=FRE (consulté le 10 Août 2014).

[322] Le *jus ad bellum* désigne : « the international law governing the resort to force by States as an instrument of their national policy ». Voir Tallinn, préc., note 45, p. 4; R. NGUYEN, préc., note 12, p. 1112-1113; Jay P. KESAN and Carol M. HAYES, « Mitigative counterstriking: self-defense and deterrence in cyberspace » **(**2011-2012**)** 25 *Harv. J. L. & Tech.* 429, p. 524-525.

[323] R. NGUYEN, préc., note 12, p. 1116.

violation puisse être reprochée à un acteur, il faut qu'il ait une qualification juridique précise (Section 1) et que cet acte puisse lui être attribué[324] (Section 2).

Section 1 : La violation des principes de droit international

Les obligations qui naissent sur le plan international sont régies par la bonne foi suivant la Charte des Nations Unies [la *Charte*][325]. Lorsque cette bonne foi est violée par un État, celui-ci commet une violation qui peut être qualifiée d'acte d'agression suivant qu'il ait fait l'usage de la force ou de simple fait illicite (Paragraphe 1). Nous analyserons si le cyberterrorisme et le cyberespionnage étatique comportent des éléments qui peuvent les intégrer dans l'une ou l'autre de ces catégories (Paragraphe 2).

Paragraphe 1 : Le principe de la bonne foi dans les relations entre États

Gérard Cornu définit la bonne foi comme un « principe fondamental du Droit des gens qui impose aux États et à leurs agents l'obligation d'agir avec esprit de loyauté dans le respect du Droit et de la fidélité aux engagements »[326]. La règle s'applique dans le geste et dans l'abstention du geste[327]. Aussi, lorsque les États se soumettent à la Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre

[324] M. CASTLE, préc., note 2, p. 3-7.

[325] CHARTE DES NATIONS UNIES, disponible en ligne : http://www.un.org/fr/documents/charter/pdf/charter.pdf (consulté le 22 Septembre 2014) [La Charte].

[326] Gérard CORNU (dir.), Vocabulaire juridique, 8ème, Paris, Association Henri Capitant, P.U.F., 2007; Pour plus d'informations, voir aussi Christine LEBRUN, *Le devoir de coopération durant l'exécution du contrat*, mémoire de maîtrise, Montréal, Faculté des études supérieures, Université de Montréal, 2012.

[327] Il faut entendre par là, l'omission prévu à l'article 2 du *Projet d'articles sur la responsabilité de l'état pour fait internationalement illicite*, UN Doc. A/56/10; GAOR, 56th Sess., Supp. No. 10 (2001) [Projets d'articles].

les états conformément à la Charte Des Nations Unies[328] [la Charte], il s'agit pour eux de chercher par tous moyens à conserver la paix et la sécurité internationale dans la continuité de l'esprit de la *Charte*[329]. La bonne foi peut donc se manifester par l'entraide interétatique ou l'absence d'usage de force contre un État (A). Suivant les grands principes du droit international, l'absence de cette bonne foi peut être caractéristique d'une violation des principes coutumiers du droit international (B).

A. La bonne foi dans les relations entre États

Rappelant le principe énoncé à l'art 2.2 de la Charte des Nations Unies, à savoir que les membres des NU « doivent remplir de bonne foi les obligations qu'ils ont assumées aux termes de la présente Charte » [Nous soulignons], la *Résolution 2625* relative aux relations amicales entre États[330] vient en clarifier le sens. L'article indique ainsi que les États ont le devoir :

> « […] de s'abstenir, dans leurs relations internationales, d'user de contrainte d'ordre militaire, politique, économique ou autre, dirigée contre l'indépendance politique ou l'intégrité territoriale de tout État »[331].

Si, par contrainte, on entend l'utilisation de la force ou la menace d'en faire usage[332] dans un sens large, un État qui enverrait des forces militaires faire des manœuvres illégales à la frontière d'un autre État[333] commettrait une violation de la bonne foi qui régit les relations internationales. Suivant le principe, les contraintes peuvent être de toute autre nature non

[328] *Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre les États conformément à la Charte des Nations Unies*, UNGA Res 2625 (XXV) UN GAOR 25th Sess, Supp No 28 at 121. UN Doc A/8028 (1971).

[329] *Id.*

[330] *Id.*

[331] *Id*. Principe 1.

[332] La Charte, art 2.4; Michael N. SCHMITT, « Cyber operations and the jus ad bellum revisited » **(**2011-2012**)** 56 *Vill. L. Rev.* 569, 572.

[333] M. SCHMITT, « Cyber operations and the jus ad bellum revisited », préc., note 327; J. P. KESAN and C. M. HAYES, préc., note 322, p. 515-518.

précisée, la constatation finale se résumant à l'atteinte à la souveraineté d'un État. Il importe donc que la manœuvre comporte un élément de coercition de nature à pousser l'autorité étatique visée à adopter une position qu'elle n'aurait pas adopté autrement. En conséquence, la mauvaise foi déséquilibrerait « la paix et la sécurité internationales »[334] établies.

Comme le souligne M. Schmitt, la contrainte peut ne pas être exercée contre un État de façon à nuire uniquement à son « indépendance politique » ou à son « intégrité territoriale »; dès lors que la souveraineté d'un État est en cause[335], la pression qui est exercée est une violation en soi de la bonne foi prévalant entre États.

Cette violation revêt plusieurs formes. Elle peut être qualifié d'acte d'agression suivant que l'on se place sous le *jus in bellum*[336] et/ou engagée la responsabilité de l'État si le fait illicite est constaté[337].

B. La violation du principe : la constitution de l'acte d'agression ou le simple fait illicite

La violation de la bonne foi entre États tombe sous l'interdiction de l'art 2.4 de la Charte des Nations Unies. Suivant la disposition :

> « Les Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies »[338].

[334] La Charte, préc., note 325, art. 1.

[335] Il peut donc s'agir d'une trouble qui affecte son peuple directement.

[336] Le *jus ad bellum* désigne l'ensemble des règles du droit international qui régissent les relations entre États. Notons en outre que la qualification d'un acte d'agression permet l'application des articles 2.4 et du chapitre VII de la Charte.

[337] Projet d'articles, préc., note 327.

[338] La Charte, préc., note 325, art. 2.4.

Comme nous l'avons vu, cette force peut être « d'ordre militaire, politique, économique ou autre […] », la seule précision étant qu'elle nuise aux éléments de la souveraineté d'un État. Aussi, l'usage de la force peut ressortir du déploiement de navires de guerre aux larges de côtes maritimes d'un État ciblé[339], ce qui serait illustratif de la mise en œuvre d'une force armée. La présence illégale des forces armées d'un État sur le territoire d'un second serait alors constitutive d'un usage prohibé de la force. Cet usage serait alors un usage direct puisqu'il implique directement une entité étatique.

Ainsi, lorsque l'usage de la force est exercé par un État contre un autre afin de lui nuire, il est considéré comme un acte d'agression directe[340]. Ce type d'acte place la violation sous l'angle de l'annexe de la *Résolution 3314 des NU* [la *résolution de Kampala*] qui définit[341] l'acte d'agression comme un usage de la force militaire exercé dans le but de contraindre un État[342]. Larry May mentionne que l'acte d'agression survient lorsqu'un État en prive un autre de sa capacité à satisfaire aux besoins de son Peuple[343]. De même, pour la CIJ, l'emploi de la force contre un État pour lui nuire est par essence une agression contre cet État[344]. Mis à part les grandes lignes de sa définition qui se borne à

[339] Voir la *Résolution 3314 (XXIX)* UNGA Res 3314 (XXIX), (14 December 1974) [Résolution 3314], p. 5. L'exemple du déploiement des navires de guerre par une force étrangère aux larges des côtes ukrainiennes par exemple. L'origine russe ne pouvant être prouvée, l'intégrité territoriale ukrainienne a été affectée et un partie de son territoire annexé à la force soviétique.

[340] C'est le cas par exemple du « blocus des ports ou des côtes d'un État par les forces armées d'un autre État ». Voir la Résolution 3314, préc., note 339, p. 5.

[341] Suivant les travaux préalables de la Résolution 3314, la définition de l'agression était impossible selon « la majorité des membres du Comité III/3, qui […], a estimé qu'une définition préalable de l'« agression » dépassait le but de la Charte et que les progrès de la technique de la guerre moderne rendaient assez difficile la définition de tous les cas d'agression ». Voir Résolution 3314 p. 1. Par la suite « [s]ur la recommandation de la Sixième Commission, l'Assemblée générale a adopté, le 31 janvier 1952, la résolution 599 (VI), dans laquelle elle a considéré qu'il était à la fois « possible et souhaitable, en vue d'assurer la paix et la sécurité internationales et de développer le droit pénal international, de définir l'agression par ses éléments constitutifs ». La Convention ne définit donc pas l'agression mais donne des indications guidant l'explication du concept.

[342] Cette définition ressort d'une synthèse faite des éléments énumérés par le texte pour désigner un acte d'agression. Pour plus d'informations, voir généralement Kevin L. MILLER, «The Kampala compromise and cyberattacks: can there be an international crime of cyber-aggression? » **(**2014**)** 23 *S. Cal. Interdisc. L.J.* 217.

[343] Larry MAY, « Aggression and crimes against peace », **(**2008**)** 319 dans Noah WEISBORD, « Conceptualizing aggression » **(**2009-2010**)** 20 *Duke J. Comp. & Int'l L.* 1 6.

[344]Military and Paramilitary Activities in and Against Nicaragua, 1986 I.C.J. 14, 65 (June 27) [Nicaragua].

punir la force militaire (cinétique) [345] , les composantes de ce « crime international suprême»[346] ne font pas l'unanimité[347].

La *résolution de Kampala*, en son amendement de l'article 8 du Statut de Rome, mentionne ceci :

> « Qu'il y ait ou non déclaration de guerre, les actes suivants sont des actes d'agression au regard de la résolution 3314 (XXIX) de l'Assemblée générale des Nations Unies en date du 14 décembre 1974 :
>
> a) L'invasion ou l'attaque par les forces armées d'un État du territoire d'un autre État ou l'occupation militaire, même temporaire, résultant d'une telle invasion ou d'une telle attaque, ou l'annexion par la force de la totalité ou d'une partie du territoire d'un autre État ;
>
> b) Le bombardement par les forces armées d'un État du territoire d'un autre État, ou l'utilisation d'une arme quelconque par un État contre le territoire d'un autre État ;
>
> c) Le blocus des ports ou des côtes d'un État par les forces armées d'un autre État ;
>
> d) L'attaque par les forces armées d'un État des forces terrestres, maritimes ou aériennes, ou des flottes aériennes et maritimes d'un autre État ;
>
> e) L'emploi des forces armées d'un État qui se trouvent dans le territoire d'un autre État avec l'agrément de celui-ci en contravention avec les conditions fixées dans l'accord pertinent, ou la prolongation de la présence de ces forces sur ce territoire après l'échéance de l'accord pertinent ;
>
> f) Le fait pour un État de permettre que son territoire, qu'il a mis à la disposition d'un autre État, serve à la commission par cet autre État d'un acte d'agression contre un État tiers ;
>
> g) L'envoi par un État ou au nom d'un État de bandes, groupes, troupes irrégulières ou mercenaires armés qui exécutent contre un autre État des actes assimilables à ceux de forces armées d'une gravité égale à celle des

[345] N. WEISBORD, préc., note 343, p. 46 ; M. SCHMITT, « Cyber operations and the jus ad bellum revisited », préc., note 332, p. 19; M. CASTLE, préc., note 35, p. 1.

[346] Judgment of the International Military Tribunal for the Trial of German Major War Criminals 421 (1946) dans N. WEISBORD, préc., note 343, p. 2.

[347] *Id.*, p. 6-8.

actes énumérés ci-dessus, ou qui apportent un concours substantiel à de tels actes. » [348]

L'étude de ses travaux préparatoires, notamment la résolution 599 (VI)[349] révèle que dans l'impossibilité de définir l'activité en elle-même, les membres de la Sixième Commission ont choisi d'énumérer des comportements pouvant être considérés comme des actes d'agression. Cette conclusion fait suite aux travaux de la Commission III/3 [350] qui affirmait que le but de la Charte serait outrepassé par la précision de tous les éléments pouvant être pris en compte mais, surtout, « que les progrès de la technique de la guerre moderne rendaient assez difficile la définition de tous les cas d'agression »[351].

L'arrêt *Nicaragua contre États-Unis* [352] a démontré que l'usage de la force pouvait également être indirecte lorsque l'État n'envoie pas ses propres organes déstabiliser un pouvoir en place[353] et qu'il agit par émissaires[354].

Par ailleurs, les applications jurisprudentielles faites par la Cour Internationale de Justice (CIJ) et le Tribunal Pénal International ont été le fruit d'interprétations larges en raison de l'obscurité du texte[355]. On note ainsi qu'au-delà de sa manifestation physique qui induit une force cinétique, l'acte d'agression peut aussi être analysé au regard des conséquences qu'il aura engendré. Il doit donc entraîner des dommages à une Nation et à un gouvernement[356]. La constatation de l'acte d'agression entraîne, suivant le droit coutumier,

---

[348] *Statut de Rome de la Cour Pénale Internationale*, July 17, 1998, 2187 U.N.T.S. 104, art 8.

[349] Elle fut adoptée par l'Assemblée Générale des NU suite aux travaux de la sixième commission ayant la charge de définir les grandes lignes d'un crime d'agression, le 31 Janvier 1952.

[350] Commission III, Résolution 3314, p. 1.

[351] *Id.*

[352] Nicaragua, préc., note 344, para. 186-189.

[353] *Id.* para 195.

[354] Les contras dans le cas présent.

[355] Ce sont en l'occurrence les arrêts Nicaragua et *Procureur c. Dusko Tadic* IT-94-1-A,;(1999), 38 ILM [Tadic] qui nous permettront de faire ressortir l'interprétation qu'en ont fait les Honorables juges de ces juridictions. Leur étude sera plus approfondie à la section suivante car elle servira à former la démonstration de l'imputabilité d'un acte à un État. Voir p. 86-87.

[356] Nicaragua, préc., note 344, para 190-191.

une défense légitime ou une contre-offensive de la part de l'État visé[357] sur autorisation du Conseil de Sécurité. Dans notre étude, nous ne nous attarderons cependant pas sur ces notions qui relèvent intrinsèquement du *jus in bellum* puisque nous privilégions la recherche d'un outil législatif commun de lutte contre les cyberattaques[358] dans une dynamique de *jus contra bellum*[359].

A l'instar de la violation de la bonne foi qu'est l'acte d'agression, la constatation du simple fait illicite révèle le non-respect d'une obligation par un État. L'article 2 du *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* [Projet d'articles] dispose :

> « Il y a fait internationalement illicite de l'État lorsqu'un comportement consistant en une action ou une omission :
>
> *a*) Est attribuable à l'État en vertu du droit international; et
>
> *b*) Constitue une violation d'une obligation internationale de l'État. »[360]

Dans l'affaire Nicaragua, le fait illicite est de nature à causer un dommage à un État et constitue donc une violation du droit international. A cet égard, la CIJ, dans ce dossier a condamné le financement et l'armement des contras par les États-Unis[361]. Cet exercice de la force est indirect puisqu'il n'ait pas le fait d'organes étatiques ou d'un État-tiers[362] sous l'influence d'un autre État.

---

[357] *Id*. ; La Charte, préc., note 325, art 51.

[358]La légifération doit pouvoir donner des outils de prévention et d'investigations pour les MSP qui soient à l'ère du temps.

[359]Yoram DINSTEIN, *War, aggression and self-defense*, Cambridge, Cambridge university press, 2005, p. 83, citant M. Howard, « Temperamenta Belli : Can War Be Controlled? » Restraints on War 1, 11 (M. Howard ed., 1979) qui illustrait son propos à partir du pacte de Kellog-Briand. Voir en ligne: http://lib.myilibrary.com/Open.aspx?id=95602 (consulté le 13 Décembre 2014).

[360]Projet d'articles, préc., note 327, art 2.

[361]Nicaragua, préc., note 344, para. 205.

[362] On entend par organe de l'État, toute entité ayant un statut bien défini dans un texte de loi national. L'article 4.2 du Projet d'articles dispose : « Un organe comprend toute personne ou entité qui a ce statut d'après le droit interne de l'État. »

Il appert évident que les cyberattaques étatiques sont des actes de violation du droit international et les notions sus-abordées nous donnent des indications qui permettent d'apprécier leur qualification propre dans une perspective de légifération. Dans cette optique, nous appliquerons les notions abordées dans ce paragraphe aux cyberattaques afin de déduire les règles internationales qui peuvent leur être appliquées. Nous l'avons mentionné dans l'introduction à ce titre 2, les cyberattaques sont des MSP dont le cyberterrorisme et le cyberespionnage étatique ont une certaine prévalence due aux défis très actuels qu'elles posent[363].

Paragraphe 2 : L'application aux cyberattaques d'origine étatique

La particularité des cyberattaques se résume à l'évidence à l'utilisation d'un outil informatique comme outil de commission. Elles redéfinissent essentiellement la notion d'usage de la force, et donc de l'acte d'agression (B). Demeurant une violation d'une obligation internationale[364], elle appelle également une analyse sous l'angle du fait illicite (A).

A. La manifeste mauvaise foi

Nous l'avons vu, la violation de l'obligation de bonne foi d'un État A se manifeste par sa volonté de nuire à un État B par divers moyens. Des modes de commission du cyberespionnage étatique et des implications telles que le désavantage économique infligé à un autre État et, dans de rares cas, la menace de possibles pertes en vies humaines[365], il est aisé de déduire la volonté de l'État acteur de nuire à l'État ciblé. Dans cette logique,

[363]De nombreux cas de cyberterorisme et de cyberespionnage étatique de toute nature ont défié la chronique ces deux dernières années. Voir quelques exemples *supra* dans le Titre 1, p. 24-29 et 36-38.

[364]Projet d'articles, préc., note 327, art 2.

[365]Voir l'attaque du Stuxnet par exemple, décrit *supra* Titre 1, p. 39.

on peut retenir que le cyberespionnage étatique et le cyberterrorisme sont des actes qui violent clairement l'obligation en cause.

Une analyse plus poussée nous permettra de faire ressortir certains éléments de la violation qui nous orientera vers la qualification de l'acte. Pour ce faire, il appert alors important de préciser les aspects de cette violation.

Primo quidem, il est intéressant de pouvoir comprendre comment une cyberattaque peut constituer une contrainte ou une menace contraignante au regard de la *Résolution 2625* des NU. Cette analyse passe par une application empirique. Prenons le cas du cyberespionnage menée contre l'Iran, présumé provenant des États-Unis, opéré à l'aide du *Stuxnet*[366]. La manœuvre[367] consistait essentiellement à voler des informations comme les encodages et les paramètres technologiques utilisés sur le site nucléaire[368]. Cette première étape ne constituait pas une réelle contrainte puisqu'elle ne mettait pas en danger la vie humaine. Elle s'assimile en fait davantage à de l'ingérence étrangère[369]. L'activité prît une pente contraignante lorsque le virus déclencha la mise en marche de certaines centrifugeuses de la base[370] dans le but de forcer la main à l'autorité dirigeante du pays.

Alio modo, la contrainte eût pour effet de causer d'importants dommages aux centrifugeuses de la base nucléaire, engendrant des réparations très coûteuses aux

[366] *Id.*

[367] *Id.*

[368] *Id.*

[369] Suivant le SCRS, l'ingérence étrangère intervient « lorsqu'une puissance étrangère manipule de façon clandestine et trompeuse des groupes au Canada dans le but d'obtenir un soutien pour ses politiques et ses valeurs, ces activités constituent une menace pour la sécurité du Canada ». Voir en ligne : https://www.csis.gc.ca/ththrtnvrnmnt/spng/frgnntrfrnc-fr.php (consulté le 10 Février 2015).

[370] Voir *supra*, p. 31-43 sur le cyberespionnage étatique.

autorités en place[371] dû au fait que l'attaque semblait être motivée par les intérêts qu'avaient les États-Unis à la fermeture du site[372].

Tertio, la violation de la bonne foi constatée[373], et acquise, il importe de s'interroger sur la qualification exacte à donner à une cyberattaque par le droit international.

B. La qualification de l'acte

La cyberattaque constitue de toute évidence une violation de la bonne foi due dans les relations publiques internationales. Cependant, est-ce qu'elle devrait être catégorisée comme un acte d'agression ou comme un simple fait illicite au regard du droit international?

Suivant l'article 2 de la *Résolution de Kampala*, l'usage de la force, caractéristique de l'acte d'agression, indique un mouvement cinétique propre au monde physique, ce qui n'est pas une réalité propre au cyberespace. Cependant, considérant les travaux préparatoires de l'adoption de la *Résolution de Kampala*, il ressort l'inexistence de consensus sur la définition de l'usage de la force justifié par la volonté de se limiter à lister diverses situations pouvant être identifiées comme telles; ceci étant expliqué par les inévitables progrès qui s'opèreraient avec l'évolution de la technologie. Les acteurs de la rédaction délibérèrent donc pour un sens large où la force était assimilée à une contrainte, épousant l'idée de la *Résolution 3314*[374].

[371] George MALBRUNOT, « De Fukushima à Stuxnet en Iran, les effets collatéraux de la cyberguerre », 4 Avril 2012, disponible en ligne http://blog.lefigaro.fr/malbrunot/2011/04/de-fukhushima-a-stuxnet-en-ira-1.html (consulté le 20 Février 2014).

[372] *Id.*

[373] Rappelons que la mauvaise foi dans les relations entre États est établie dès lors qu'un État A cherche à nuire de quelque façon que ce soit à un État B. Dans le cas décrit ci-dessus, le vol d'informations confidentielles et les dommages causés par l'infiltration du maliciel étaient de nature à causer du tort au gouvernement iranien. De fait, ces actes contrevenaient à l'article 2.2 de la Charte des Nations Unies.

[374] Résolution 3314, préc., note 339, p. 1.

De fait, les États-membres de la Sixième commission[375], en connaissance de cause se cantonnèrent aux réalités de leur temps. A cet égard, l'internet représente une technologie utile aux forces d'un État. Il s'intègre dès lors à la logique du progrès moderne qu'avançaient les membres de ladite Commission. Le cyberterrorisme et le cyberespionnage d'origine étatique consistent en des attaques informatiques dont la principale arme utilisée est un maliciel, qui n'implique quasiment aucune force physique de frappe lorsqu'elle est exclusivement menée via le numérique[376]. En outre, cet usage de la force non-cinétique peut engendrer des pertes pour un État lorsqu'elle a pour finalité l'interruption des communications d'une tour de contrôle aéroportuaire[377]. Pour retenir la présence d'un usage de la force, il faut qu'il entraîne des dommages d'ordre économique, politique et des retombées préjudiciables pour la population civile[378]. Rappelons-nous le cas de la cyberattaque menée contre la Géorgie[379], le gouvernement a été ramené à une époque préindustrielle[380] et a subi de sérieuses pertes économiques dû à l'impossibilité d'accéder à des sites gouvernementaux[381]. Les cyberattaques dans leur globalité peuvent être considérées comme des actes d'agression si l'on entend que la présence exclusive d'une force cinétique ne conditionne pas la qualification d'un acte d'agression.

Dans cette même logique, selon Blank, les cyberopérations peuvent être considérées comme des actes d'agressions propres au cyberespace. Il affirme:

---

[375] *Id*., p. 2.

[376]En effet, dans un cas hypothétique, la cyberattaque peut être menée pour faciliter une attaque physique. Il peut s'agir du blocage du système informatique d'un aéroport pour ensuite attaquer un avion. De fait, l'absence de force cinétique est relative lorsque l'attaque informatique est suivie d'une attaque armée. Cette situation soulève deux éléments juridiques, à savoir la qualification de deux actes distincts.

[377] Voir *supra* les exemples de MSP qui témoignent de leur dangerosité, Titre 1, p. 13-43.

[378] L'article 2.4 de la Charte indique que les effets de l'usage de la force soient de nature à ébréché la paix et la sécurité internationale.

[379] N. WEISBORD, préc., note 343, p. 19.

[380]*Id.*, p. 20; M. SCHMITT, « Cyber operations and the jus ad bellum revisited », préc., note 332, p. 571.

[381] N. WEISBORD, préc., note 343, à la p. 20, l'auteur écrit: « Government, media, communications and transportations companies were attacked. The website of Georgian president Mikheil Saakashvili was overwhelmed by a "denial of service attack" whereby a barrage of millions of bogus requests overloaded and shut it down. »

> « […] any cyber action against critical national infrastructure should qualify as an armed attack, or, alternatively, to an "instrument based" approach, according to which a cyber operation constitutes an armed attack if "the damage caused by a cyber attack could previously have been achieved only by a kinetic attack »[382].

De même, suivant le Manuel de Tallinn[383], les cyberattaques qui touchent directement des infrastructures essentielles peuvent être considérées comme des usages de la force lorsqu'on considère l'ampleur des dommages causés[384]. M. Schmitt établit dans son article 7 points d'analyse[385] menant à la catégorisation des cyberattaques comme acte d'agression. En se basant sur le cas de l'Estonie, l'auteur démontra que les cyberopérations comportent des éléments d'identification les reliant fortement à la notion d'usage de la force sans que le processus fût le même[386].

Considérant que toutes les cyberattaques n'impliquent pas forcément une force armée ni une destruction physique de biens comme ce fut le cas par exemple en Estonie ou au Tibet ou même en Iran, un doute subsiste sur leur classification dans ce type d'actes. C'est d'ailleurs en ce sens que le Manuel de Tallinn précise : « They [The international Group of Experts] also agreed that act of cyber intelligence of cyber gathering and cyber theft, as well as cyberoperations that involve brief or periodic interruption or non-essential services »[387] ne peuvent être qualifiés d'acte d'agression.

---

[382] Laurie K BLANK, « International Law and Cyber Threats from Non-State Actors », **(**2013) 89 *Int'l L. Stud. Ser. US Naval War Col.* 415.

[383] Tallinn, préc., note 45, p. 54.

[384] M. SCHMITT, « Cyber operations and the jus ad bellum revisited », préc., note 332, p. 5-8 ; Tallinn, préc., note 45, p. 54; Nicaragua, préc., note 344, para 191; L. BLANK, préc., note 382, p. 415.

[385] Ce sont la sévérité, l'immédiateté, l'impact exact direct ou indirect, le degré de destruction, l'avancée de l'invasion, la possibilité de la légitime défense et l'attribution de l'acte. Voir M. SCHMITT, « Cyber operations and the jus ad bellum revisited », préc., note 332, p. 7.

[386] *Id.*; Pour plus d'informations sur la cyberattaque menée contre l'Estonie, voir N. WEISBORD, préc., note 343, p. 20.

[387] Tallinn, préc., note 355, p. 55.

En effet, les cyberopérations dont l'ampleur ou les effets[388] ne sauraient s'assimiler à ceux d'un usage de la force cinétique laisse planer le doute sur leur qualification dans cette catégorie[389]. Ainsi, la question de la qualification n'étant pas entièrement résorbée, la constatation du simple fait illicite semble solutionner le problème.

En ce sens, se fonder uniquement sur l'existence de la violation d'une obligation internationale pour définir une cyberopération illégale semble plus approprié puisqu'il est avéré que leurs effets et leurs gravités sont très aléatoires. Demeurer dans la généralité du fait illicite permet en autre d'étudier avec soin chaque cas de cyberattaques.

Cette distinction ne joue cependant pas sur l'attribution d'un acte à un État et donc, sur sa responsabilité. Dans la section qui suit, nous verrons les principes internationaux de l'imputabilité d'un acte à un État.

Section 2 : L'imputabilité à un État

En droit international, l'acte d'agression ou le fait illicite implique la responsabilité collective d'un État[390]. Cependant, pour que celle-ci soit engagée il faut que l'acte en question puisse lui être attribué[391]. Plusieurs cas de figures permettent de déterminer l'imputabilité d'un acte à un État. Ils peuvent varier suivant que l'État ait impliqué ses propres organes gouvernementaux ou qu'il ait participé au financement de la contrainte. Sa responsabilité peut également être engagée par le fait d'acteurs non-étatiques[392]. Pour faire ressortir les critères applicables à chaque effet, nous étudierons l'imputabilité directe

[388] Nicaragua, préc., note 344, para 195; Pour mesurer la gravité d'une cyberopération, il est intéressant de consulter le tableau publié par le SP sur les MSP, voir note 276.

[389] M. Schmitt estime quant à lui que : « For example, current understandings of the terms "use of force," "armed attack," and "attack," which are based in part on the nature (as distinct from the severity) of an act's consequences, are certain to prove wanting in tomorrow's wired social construct […] ». Voir Michael SCHMITT, « Cyberspace and international law: the penumbral mist of uncertainty », préc., note 5, p. 180.

[390] Résolution 3314, préc., note 339; La Charte, préc., note 325, art 2.4.

[391] M. CASTLE, préc., note 35, p. 6.

[392] *Id.*

et indirecte d'une cyberattaque à un État (Paragraphe 1). Par la suite, nous aborderons l'épineuse question de la preuve (Paragraphe 2).

Paragraphe 1 : L'imputabilité d'une cyberattaque à un État

Lorsqu'un État est à l'origine d'une cyberattaque, et qu'il viole son obligation de ne pas troubler l'ordre et la paix au niveau planétaire, il engage sa responsabilité en vertu du droit international[393]. Il peut par ailleurs arriver que cette responsabilité lui incombe lorsqu'elle émane de son territoire sans que son infrastructure étatique y soit mêlée. Seront donc abordées dans un premier temps la responsabilité de l'État suivant le degré de contrôle qu'il exerce (A) et, dans un second temps, seront abordées les actes de particuliers qui engage sa responsabilité (B).

A. L'attribution d'une cyberopération à un État

La responsabilité directe d'un État peut être engagée suivant la *Résolution de Kampala* qui énonce qu'un État est coupable d'un acte d'agression dès lors que sont impliqués ses agents officiels; que ce soit ses organes gouvernementaux, ses forces armées ou ses services secrets. Ces organes ou infrastructures doivent avoir un statut bien défini par le droit interne du pays[394]. De fait, un État A qui invoque la responsabilité d'un État B dans la commission d'une cyberopération illégale devra démontrer que ce sont les agents du second qui ont œuvré. La charge reviendrait alors à l'autre État de prouver que ceux-ci ont agi sans son accord officiel[395]. Si les investigations de la cyberattaque menée contre

[393] La Charte, préc., note 325, art 2.4 ; Projet d'articles, préc., note 327.

[394] M. CASTLE, préc., note 35, p. 6; Projets d'articles, préc., note 327, art 4-5.

[395] Projets d'articles, préc., note 327, art 7; M. CASTEL, préc., note 35, p. 6.

l'Estonie avaient uniquement révélé une adresse électronique d'un membre du gouvernement Russe, la responsabilité de cet État aurait par exemple pu être retenue[396].

Outre l'implication directe de son infrastructure numérique, l'État peut également être tenu responsable s'il avait connaissance et avait admis sur son sol, la préparation de l'activité illégale contre un État par un groupe terroriste, un particulier ou autre destiné à infliger des pertes économiques ou humaines via le numérique; tout ceci en violation de l'art 2.4 de la *Charte*[397].

Par ailleurs, le degré de contrôle qu'un État exerce sur des organes ne relevant pas directement de sa compétence en vertu du droit local détermine aussi l'imputabilité de l'acte. En ce sens, l'article 8 énonce que cette responsabilité peut être engagée si les personnes ou groupes de personnes agissent « sur les instructions ou les directives ou sous le contrôle de cet État »[398]. Ici, le degré de contrôle est relatif aux instructions reçues mais aussi à la fourniture d'armes. A cet égard, la CIJ dans l'affaire *Nicaragua* a statué que le financement, l'armement ainsi que l'indication de stratégie constituait un degré de contrôle suffisant pour engager la responsabilité d'un État[399]. Afin de déterminer le degré de contrôle qu'un État exercerait sur une entité cyberterroriste, il faudrait prouver que celle-ci recevait de sa part de l'aide technologique et des directives précises. Résultat quasi-impossible. Dans un article de journal, E. ERCOLANI affirmait : « […] la Russie aurait loué temporairement les services de propriétaires de botnets, des réseaux de PC zombies, pour accroître le nombre d'ordinateurs impliqués dans l'attaque en déni de service lancée contre l'Estonie. Environ un million d'ordinateurs auraient donc été mis à contribution »[400]. Il semblerait alors que la Russie aurait eu un contrôle effectif sur la

[396] Pour plus d'informations sur le cas de l'Estonie, voir note 386.

[397] La violation serait ainsi avérée en raison des effets d'une éventuelle cyberopération impliquant des pertes en vies humaines. Les effets d'un usage de la force cinétique seraient alors similaires à ceux issus de ladite cyberattaque.

[398] Projet d'articles, préc., note 327, art 8.

[399] Nicaragua, préc., note 344, para 188; Voir aussi Tadic, préc., note 355, para. 81-94.

cyberattaque et pourrait être reconnue coupable de son implication dans la commission d'un fait illicite[401].

A l'instar de cette responsabilité qui ressort de l'implication avérée de l'État, un individu ou un groupe de personnes peut engager, par ses actes, la responsabilité d'un État.

B. La responsabilité de l'État par le fait d'acteurs non-étatiques

Cette responsabilité trouve sa légalité en droit international dans le *Projet* d'articles qui, rappelons-le, énonçait que la responsabilité de l'État pouvait être engagée par omission[402]. M. Castle écrit:

> « However, even if a state is not involved directly or indirectly in a cyberattack, it has certain obligations towards the targeted state. There is a duty on its part to prevent such hostile action by private parties when originating from servers and actors located within its physical boundaries. This duty includes preventing the cyber attack and, if that is too late or impossible, attempting to identify the actors, and bringing to justice all those who tried to disrupt or damage the systems of the targeted state »[403].

Un État, en vertu du principe de précaution[404], doit déployer les efforts nécessaires pour contenir tout risque contre un autre État lorsqu'il en a connaissance[405]. Ce risque peut être par exemple une préparation de groupes armés sur son territoire dans le but de mener une

---

[400] Voir Emilien ERCOLANI, « La Russie impliquée dans la cyber-attaque contre l'Estonie ? », 4 Juin 2007, disponible en ligne : http://www.linformaticien.com/actualites/id/2168/la-russie-impliquee-dans-la-cyber-attaque-contre-l-estonie.aspx (consulté le 13 Février 2014).

[401] Le fait illicite serait retenu ici à cause de l'ampleur de l'activité et des dégâts recensés qui ne sont pas physiques. Nous nous garderons toutefois de tenir ce raisonnement en raison de l'absence de preuves concrètes et avérées de l'implication de la Russie.

[402] Projet d'articles, préc., note 327, art 2.

[403] M. CASTLE, préc., note 35, p. 10.

[404] Pour plus d'informations sur le principe de précaution, voir : Jonathan B. WIENER, Michael D. ROGERS, James K. HAMMITT et Peter H. SAND, *The reality of precaution Comparing risk regulation in the United States and Europe*, Washington D.C., RFF Press, 2011.

[405] C'est le cas dans l'affaire du *Détroit de Corfu Royaume-Uni* contre *Albanie*, [1949] ICJ Rep 4 [*Corfu*] para. 22; Voir aussi *France* v. *Turkie* 1927 PCIJ (Ser A) No 10 para. 88.

offensive contre un État[406]. L'abstention a également été invoquée dans l'affaire *Tadic* dans laquelle les juges du TPIY ont jugé que la responsabilité de l'État était engagée puisque celui-ci n'avait pas exercé un contrôle adéquat sur les belligérants[407].

Dans le cas de l'Estonie où le coupable fut désigné comme un « loup solitaire » n'agissant sur aucun ordre, il semble que le pays touché aurait pu prétendre à un dédommagement de la part de la Russie puisque la faute avait été commise par l'un de ses ressortissants[408]. En effet, lorsque la responsabilité de l'État est retenue pour un acte commis par des belligérants sur son territoire, il est tenu d'obliger lesdits belligérants à arrêter leur acte, et à s'engager à ne plus récidiver. L'État est tout de même tenu d'offrir des dédommagements à l'État visé. Toute poursuite contre un État ne peut cependant pas se mettre en branle sans les preuves de son implication[409].

Paragraphe 2 : L'épineuse question de la preuve

Pour pouvoir engager des poursuites ou, tout le moins prouver qu'un État est auteur direct ou indirect d'une cyberattaque, il faut pouvoir lui attribuer l'acte en cause. La preuve est indispensable à toute imputabilité[410]. Dans le cas des crimes internationaux et, en l'occurrence, des actes d'agression, la constatation de la présence des forces portant l'uniforme officiel est par exemple un signe distinctif[411]. Cette obligation est très difficile

[406] *Corfu*, préc., note 405, para 22.

[407] L. K. BLANK, préc., note 382, p. 642.

[408] L'identité du coupable n'est pas connu mais, selon la presse, il s'agirait d'un jeune homme russe de 30ans. La justice estonienne l'aura condamné à 1100 euros d'amende. Voir en ligne : Guerric PONCET, « Condamnation d'un Russe pour cyber-attaque contre l'Estonie », 25 Janvier 2008, disponible en ligne : http://www.lepoint.fr/actualites-technologie-internet/2008-01-25/condamnation-d-un-russe-pour-cyber-attaque-contre-l-estonie/1387/0/220620 (consulté le 10 Décembre 2014).

[409] Michael N. SCHMITT, « Classification of Cyber Conflict » **(**2013**)** 89 *Int'l L. Stud. Ser. US Naval War Col.* I. 235. L'auteur mentionne que l'application de ce principe de droit international est variable suivant l'espèce.

[410] M. CASTLE, préc., note 35, p. 6.

[411] Il est intéressant de remarquer comment la Russie a contourné cet aspect en envoyant des forces sans uniforme indicatif de la provenance de ces forces.

à remplir de la part de l'État victime, la dématérialisation du cyberespace ne permettant pas de retracer avec précision l'origine d'une attaque informatique. Il se pose alors la question de la preuve numérique (A) qui en soulève une autre, celle de la difficulté de l'attribution d'une cyberattaque à un État (B).

A. La preuve numérique : un problème ardu

Plusieurs épisodes de cyberattaques ont été relatés par la littérature scientifique au cours de ces dernières années[412]. Celle menée par le directeur de l'IUT, Ronald Deibert, dans le cadre de son enquête sur le *Ghosnet*[413], met en exergue des éléments de preuve qui permettent de retracer une cyberattaque et de pouvoir, de façon très globale situer son point d'origine.

Pour le cyberespionnage étatique, la méthode utilisée par les enquêteurs du *Ghosnet* partait de la détermination du champ d'investigation, c'est-à-dire de la détermination du code-source du virus et son fonctionnement, et de la recherche contextuelle qui comprend, en fonction des cibles touchés par la manœuvre, l'étude du contexte géopolitique, le type d'informations collectées et le temps global alloué de l'attaque[414]. La définition du champ de l'enquête aura permis de porter une attention sur le réseau wifi d'une ONG espionnée, le Common Ground[415]. Suite à la détection de l'activité d'un maliciel, les techniciens auront simplement eu à isoler ses fonctionnalités :

> « [t]ennorNet was also captured, revealing malicious activity. An anomaly was detected when analyzing this traffic: computers in Dharamsala were

[412] L. K. BLANK, préc., note 382, p. 5-10.

[413] Tracking the Ghosnet, préc., note 27, p.14.

[414] Le temps alloué à l'attaque comprend la durée estimée de la conception du maliciel, du lancement de l'attaque et du temps de l'espionnage. Shadows, préc., note 140, p. 14.

[415] *Id.*

> beaconing or checking in with a command and control server (jdusnemsaz.com/119.84.4.43) located in Chongqing, PRC »[416].

Cela aura permis de retracer l'origine approximative de l'attaque en localisant les différents réseaux où se retrouvait le code-source du virus : « [t]he location of Chongqing is contextually interesting as it has a high concentration of Triads — well known Asian-based organized criminal networks — who have significant connections to the Chinese government and the Chinese Communist Party »[417].

L'investigation purement technique prît en compte les noms de domaines qui servaient de base de contrôle des maliciels, les types de maliciels, les données volées, mais surtout, servir à faire le tracé des différents systèmes de noms de domaine (Domain Name System, ci-après DNS) qui aura conduit à situer le centre névralgique de l'espionnage[418]. Notons que les DNS sont des plateformes cybernétiques de commande et de contrôle de maliciel qui servent de base aux agents des attaques[419]. Les investigations pour tracer le *Ghosnet* ont permis de définir une région géographique précise d'origine du maliciel : la Chine, plus précisément un des départements de ses services secrets situés sur l'île d'Hainan[420].

Dans ce cas d'espionnage par le *Ghosnet*, bien que la majorité des liens aient conduit à l'implication des autorités chinoises[421], celles-ci démentirent toute implication dans la vaste opération d'espionnage.

Du côté de l'Estonie, les preuves récoltées indiquaient l'implication de membres du gouvernement Russe : « Le 30 avril, le ministre de la justice estonien affirmait que l'adresse Internet utilisée lors d'une attaque appartiendrait à un membre de

---

[416] *Id.*

[417] *Id.*

[418] *Id.*, p. 10-11.

[419] *Id.*, p. 13; Pour plus d'informations sur les DNS, consulter en ligne : Palo Alto Networks DNS protection mecanisms, disponible en ligne : http://fr.slideshare.net/MarcelloMarchesini/dns-protection (consulté le 17 Février 2015).

[420] Tracking the Ghostnet, préc., note 27, p. 30-32 ; Voir Titre 1 *supra*, p. 39-43.

[421] Voir Titre 1 *supra*, p. 38-43.

l'administration du Président russe, Vladimir Poutine »[422]. De plus, selon l'Asymetric Threats Contingency Alliance (ATCA)[423] qui pointe les ressources utilisées :

> « The attackers used a giant network of bots (enslaved computers) on 9th May -- perhaps as many as one million slave computers in places as far away as North America and the Far East -- to amplify the impact of their assault. In a sign of their financial resources, there is evidence that they rented time from trans-national criminal syndicates on Botnets ».[424] [Nous soulignons]

Rappelons que l'infrastructure utilisée et les ressources financières contribuent à indiquer la réelle ampleur d'une cyberattaque, son origine et ses objectifs.[425] Dans le cas de l'Estonie, les preuves indicielles que sont l'adresse IP et le coût de la cyberopération orientent les soupçons vers l'État Russe.[426]

En définitive, les principales preuves qui semblent pouvoir être avancées dans une cyberattaque sont l'identification des maliciels utilisés, les bases de contrôle et de commande qui servent à diriger le maliciel et à recueillir les informations et/ou le coût estimé de l'opération.

Dans les cas étudiés ci-dessus, les deux États nièrent leur implication. Cependant, à la lumière des indices relevés lors de l'enquête, la perspective d'un nouveau mode de preuve à l'échelle internationale semble se concrétiser. C'est en ce sens que la *Convention de Budapest* peut aider en fournissant d'importants éléments d'orientation d'un cadre légal

---

[422] M. SCHMITT, « Cyber operations and the jus ad bellum revisited », préc., note 332, p. 2-3; John MARKOFF, « Before the Gunfire, Cyberattacks »**,** 13 Août 2008**,** N.Y. TIMES, disponible en ligne : http://www.nytimes.com/2008/08/13/technology/13cyber.html (consulté le 13 Février 2015).

[423] L'ATCA est une initiative d'experts philanthropes mis sur pied par le mi2g en 2001 afin d'aider à comprendre les défis internationaux actuels. Pour en savoir plus sur le mi2G, voir en ligne la page d'accueil de l'institution http://www.mi2g.com/ (consulté le 17 Février 2015).

[424] ATCA briefings, « Cyber Warfare– Beyond Estonia-Russia ATCA Briefings The Rise of China's 5th Dimension Cyber Army », 3 Mai 2007, disponible en ligne http://www.mi2g.com/ (consulté le 15 Février 2015).

[425]Voir Titre 1 *supra*, p. 31-43 sur le cyberespionnage.

[426]L'implication de cet État n'étant pas certaine, les rédacteurs du Manuel de Tallinn se sont limités à dresser les grandes lignes de l'application du droit international à une cyberguerre dans une logique de prévention. Voir : Tallinn, préc., note 45.

international de lutte contre les menaces de la paix que constituent les cyberopérations destinées à affaiblir une Nation[427]. Nous apprécierons cet apport dans le chapitre suivant.

Ce silence législatif ne permet pas d'indexer à proprement parler l'implication d'un État dans une cyberattaque, le faire, se baserait sur de simples présomptions. La collecte de ces indices étant d'autant plus ardue dans le cyberespace.

B. La difficulté de l'attribution d'une cyberattaque à un État

Les cyberattaques ayant ou pas un faible seuil de gravité ne nécessite pas l'utilisation de maliciels coûteux ou le déploiement d'effectifs humains importants. Que ce soit dans le cyberterrorisme ou le cyberespionnage étatique, les outils de commission demeurent assez similaires. De plus, ces maliciels et leur mode d'emploi sont disponibles quasiment sans frais sur certains sites web[428]. Lorsqu'elles ont des visées destructrices, elles passent par l'utilisation des DDoS et de PC zombies qui brouillent l'origine réelle de l'acte[429]. Il n'est pas donc possible de définir clairement la responsabilité de l'auteur d'une cyberattaque. L'utilisation de nombreux intermédiaires exacerbée par la dématérialisation de l'environnement ne permet pas de récolter les preuves sur un terrain précis.

La collecte d'éléments indicatifs et concordants permettant de déterminer l'implication d'un État requiert par ailleurs des connaissances informatiques et techniques très précises car, le cyberespace défit les limites spatiales qui entraînent de gros risques de confusion dans la collecte[430].

Au bout de notre étude du droit international, beaucoup de questions demeurent sans réponses claires. En effet, au regard de l'étude du *jus ad bellum* qui semble être

[427] Nous étudierons la convention de Budapest *infra* à partir de la page 92, les différents apports à la communauté internationale que révèle l'étude de la *Convention de Budapest*.

[428] I. AWAN et B. BLACKEMORE, préc., note 75, p. 30.

[429] Comme ce fut le cas de l'Estonie par exemple, note 386.

[430] L. K. BLANK, préc., note 382, p. 415.

actuellement le seul droit susceptible de donner sa qualification aux cyberattaques en général[431], y a-t-il d'autres voies possibles de lutte légale contre ces cybermenaces?

La Convention de Budapest, ayant une exclusive vocation pénale s'adresse aux acteurs non étatiques des cyberattaques. Elle définit des lignes procédurales au sein de chaque État visant à prévenir les cybercrimes ayant un seuil de gravité minimal[432]. A son étude, il est aisé d'en déduire des indicateurs d'une législation transnationale de la cybersécurité à mettre en place en temps de paix, au sein de chaque pays et qui pourrait de fait s'appliquer aux cybermenaces de type 1[433].

Chapitre 2 : La Convention de Budapest : dans la dynamique transfrontalière de lutte contre les cyberattaques

L'élaboration de la convention européenne a connu deux étapes majeures de réflexion sur la cybercriminalité par le Conseil des Ministres européens[434]. Constatant l'absence de cadre légal international[435] confrontant les crimes liés à l'ordinateur et à l'internet[436], le

[431] « The Tallinn Manual on the International Law Applicable to Cyber Warfare is not an official document, but instead an expression of opinions of a group of independent experts acting solely in their personal capacity ». Le Manuel de Tallinn s'inspire de deux manuels à savoir « *San Remo Manual on international law applicable to armed conflicts at sea* » et du « *Manual on international law applicable to air and missile warfare* ». Il a rédigé par des experts en quête d'une réponse sur la qualification juridique des cyberattaques. Tout au long de leur rapport, ils évaluent les différentes applications possibles du droit humanitaire international aux attaques informatiques. La gravité de la situation de l'Estonie leur a imposé ces réflexions qui apportent aujourd'hui certaines indications sur les natures des cyberattaques au plan international et comment, en cas de guerre informatique (cyberwarfare), la communauté internationale peut élaborer des contre-offensives. Voir Tallinn, préc., note 45.

[432] Voir Titre 1 *supra*, p. 56-61.

[433] J. P. KESAN and C. M. HAYES, préc., note 322, à p. 520, l'auteur mentionne: « We argue that the ECC could potentially provide a framework to address international cybercrime issues. However, the relatively low participation in the ECC and the difficulty of enforcing the ECC's provisions prevent it from being an acceptable solution to the problem of cyberattacks across international borders. »

[434] CONSEIL DE L'EUROPE, Rapport explicatif de la *Convention sur la cybercriminalité STE n°185*, 8 Novembre 2001, p. 2-5, disponible en ligne http://conventions.coe.int/treaty/fr/Reports/Html/185.htm (consulté le 20 Septembre 2014) [Rapport explicatif].

[435] CONSEIL DE L'EUROPE, *Recommandation N° R (89) 9* (adoptée par le Comité des Ministres le 13 septembre 1989), disponible en ligne :

Conseil mis sur pied le Comité d'experts sur la cybercriminalité (PC-CY)[437] en 1997[438] qui rédigea la Convention européenne signée à Budapest en 2001[439]. Dans ce domaine, la Convention représente le texte juridique le plus fédérateur[440] au plan international. Une prospective de la cybersécurité adéquate à la répression des cyberopérations majeures ne peut se faire sans l'étude de ces dispositions conventionnelles.

Par ailleurs, cette recherche d'une législation internationale sur la qualification juridique de ce type d'actes répondra au besoin d'une amélioration de la cybersécurité canadienne à appliquer au plan national. Il importe donc, dans notre recherche, de toucher à ce volet des relations internationales, c'est-à-dire aux outils de coopération internationale utiles à toute lutte efficace dans la dimension cybernétique.

C'est à cette fin que dans le premier chapitre de cette partie, sera abordée l'étendue de la Convention de Budapest utile à notre démarche (Section 1). Dans le contexte canadien, l'application de ces directives se heurte à des enjeux variés qui portent, entre autres, sur la situation juridique nationale et le mécanisme de coopération internationale dans le domaine de la défense nationale. Afin d'évaluer les implications d'une uniformisation au plan international, il sera donc question, dans le second chapitre, de l'effectivité de la démarche d'uniformisation cybersécuritaire appliqué au Canada (Section 2). Ce cheminement nous permettra de montrer que l'uniformisation juridique des cyberstratégies gouvernementales est une panacée dans la lutte contre les cybercrimes

---

https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900321&SecMode=1&DocId=702360&Usage=2(consulté le 13 Août 2014) [Recommandation n°89].

[436] Rapport explicatif, préc, note 434, p. 3.

[437] Le PC-CY désigne le « Comité d'experts sur la criminalité dans le cyber-espace ». Voir : Rapport explicatif, préc., note 434, p. 3.

[438] A. WEBER, préc., note 48, p. 430.

[439] La Convention a été signée par des États non-membres de la communauté européenne dont les États-Unis et le Canada. Les autres États non-membres sont l'Afrique du Sud et le Japon.

[440] Elle regroupe plus de 55 signatures dont celles de six pays non européens. Pour plus d'informations sur la liste des pays signataires, voir CONSEIL DE L'EUROPE, Bureau des Traités, Convention sur la cybercriminalité, 23 Novembre 2001, STE n°185, disponible en ligne : http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=FRE (consulté le 10 Août 2014).

d'envergure en dépit des différents enjeux que pose la coopération internationale dans le domaine.

Section 1 : Les éléments des infractions typiquement numériques assimilables au cyberterrorisme et au cyberespionnage étatique

Nous l'avons vu, les cyberopérations peuvent être considérés comme des usages de la force au regard des conséquences qu'elles engendrent[441]. Pour obtenir la qualification de fait internationalement illicite, il importe de pouvoir énumérer les différentes infractions qui le constituent. En ce sens, la Convention de Budapest permet d'entrevoir les différents éléments d'une infraction numérique qu'il est possible de prendre en compte en l'espèce (Paragraphe 1).

Elle définit également des pouvoirs procéduraux à mettre en place au niveau de chaque instance nationale afin de prévenir et de réprimer les acteurs non étatiques coupables de ces méfaits. Ceux-ci sont utiles à la collecte des indices destinés à indiquer le coupable du crime (Paragraphe 2).

Paragraphe 1 : Les éléments constitutifs des cyberattaques majeures

Il ne semble pas utile de rappeler que des cyberopérations telles que le cyberespionage étatique et le cyberterrorisme représentent au prime abord des crimes informatiques puisqu'ils débutent par une intrusion dans un système informatique auquel ils n'ont normalement pas accès. De fait, la Convention de Budapest vient indiquer les termes exacts du premier stade de la violation. Ainsi, en ses articles 2, 5 et 6, elle énumère des infractions propres aux deux types de cyberattaques retenues (A) et en ses articles 3 et 4, des infractions qui n'entrent pas systématiquement dans la constitution de ces crimes (B).

[441] Tallinn, préc., note 45, p. 54 ; N. WEISBORD, préc., note 343, p. 46.

A. L'apport des articles 2, 5, 6

Les articles 2, 5 et 6 évoquent respectivement la répression de l'accès illégal à des données et à des systèmes informatiques, le préjudice à un système informatique et l'utilisation d'outils informatiques à des fins malveillantes.

« L'accès illégal » peut s'effectuer par l'entrée dans un système informatique via internet pour accéder à un intranet ou d'un intranet pour accéder aux protocoles TCP/IP d'une entreprise. Il consiste également à pénétrer dans les serveurs d'un quelconque organisme afin de subtiliser des données ou de les altérer. L'infraction est constituée lorsqu'une personne entre sans autorisation dans un système informatique dans le but de subtiliser de l'information ou de passer au travers pour atteindre un autre système informatique à des fins illicites. Elle constitue une menace à l'équilibre de l'exploitant du système, en altérant sa sécurité, que ce soit au niveau de « sa confidentialité, de son intégrité et de sa disponibilité ».

La première étape de commission de l'acte passe par un accès illégal d'un serveur ou d'un réseau internet, « intranet » ou « extranet » lorsque celui-ci est utilisé comme outil[442]. Lorsque le réseau est, dans un autre cas, la cible[443], l'auteur y accède en utilisant un autre système informatique qui lui permettra d'atteindre la cible informatique finale. Le processus de la commission de l'acte peut varier suivant la manœuvre utilisée par les contrevenants. Ainsi, elle peut, par exemple, passer par l'intrusion d'un maliciel qui servirait de pont de passage entre le système informatique et celui de l'auteur de l'acte. Si l'accès illégal est constitué dans les cybercrimes que sont le cyberterrorisme et le cyberespionnage étatique, il n'en constitue que la première étape de commission puisqu'elle est annonciatrice d'une atteinte à l'intégrité du système et celle des données informatiques par l'utilisation de maliciels.

[442] Voir *supra* Titre 1 les cas où l'internet est utilisé comme outil, p. 25.

[443] *Id*., l'internet est utilisé comme cible lorsque la manœuvre vise à interrompre des lignes du réseau d'infrastructures essentielles. Le procédé consiste le plus souvent en la provocation de dénis de service.

La corruption de tout mécanisme assurant le traitement de données informatiques est punie par l'article 5 de la convention qui prescrit à chaque État d'adopter des dispositions pour punir « l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques ». Aussi, pour être constituée, elle doit être commise avec l'intention d'empêcher illicitement l'accès ou l'utilisation normale faite d'un système informatique; elle constitue dès lors une entrave à son fonctionnement. L'atteinte la plus récurrente à l'utilisation normale et légitime d'un système informatique est l'envoi de déni de service qui a pour effet de saturer les serveurs des exploitants par l'envoi massif de requêtes en passant par un réseau informatique[444].

Dans le cas de la cyberattaque contre l'Estonie évoqué plus haut, la manœuvre des dénis de service fut utilisée pour bloquer toute utilisation qui pouvait être faite des serveurs ou des services informatiques sur la totalité du territoire[445]. Un préjudice peut également être porté à un système informatique de traitement de données par une agression physique contre ses serveurs mais cet acte serait exclu de la catégorisation de cyberattaque puisque le canal de commission n'est pas un outil informatique[446].

Le cyberterrorisme est une infraction punissable au sens de l'art 5 de la convention puisque son but premier est la destruction des actifs essentiels d'un État. Il en est de même pour le cyberespionnage étatique dans lequel les auteurs peuvent non seulement accéder illégalement aux données ou au système informatique mais peuvent en plus, modifier les informations enregistrées dans le code de paramétrage des dispositifs informatiques.

Toutes ces infractions sont commises à l'aide de logiciels malveillants mis à la disposition des internautes ou de personnes spécifiques ou créés et utilisés à la seule fin de nuire à

[444] C'est le procédé le plus répandu d'attaques cybernétiques surtout lorsqu'il s'agit de cyberterrorisme.

[445] B. GAGNON, préc., note 8.

[446] Il s'agirait plutôt de technoterrorisme. Nous avons abordé cette notion *supra* à la page 24, note 111.

l'autorité étatique ou d'entraver la bonne utilisation des systèmes informatiques[447]. En vue de freiner cette dérive, la convention encadre la pénalisation de ces actes de mise à disposition en son article 6. La Convention punit les infractions d'envergure que sont le cyberterrorisme et le cyberespionnage étatique suivant les articles 2, 5 et 6 mais les articles 3 et 4 sont plus spécifiques à chaque cas de MSP.

B. L'apport de la Convention en ses articles 3 et 4

L'article 3 consacre la pénalisation de l'interception d'informations confidentielles dont l'accès est soumis à une autorisation préalable. C'est le cas par exemple du rapport sur les techniques de torture exécutées par la CIA[448]. Si la version complète du rapport, soit 6700 pages, se retrouvaient publier suite à un accès illégal au support informatique où il est sauvegardé, l'infraction d'interception d'informations confidentielles serait constituée. L'infraction constituée par l'interception d'informations peut se faire avec des moyens informatiques ou « techniques », qui servent à l'extraction des données d'un système informatique ou à la mise en place de logiciels permettant de récolter de l'information. Dans une situation où intervient une communication professionnelle entre deux employés au sein du SP sur une question relevant de la sécurité intérieure, l'interception de ces échanges non publics aggraverait par exemple la qualification de l'infraction due à la nature des renseignements volés.

L'infraction, ainsi constituée, s'inscrit dans le schéma de commission du cyberespionnage étatique. En effet, l'interception par l'utilisation de « matériel technique » pour extraire des données informatiques s'assimilerait à une interception par écoute téléphonique illégale. L'infraction englobe à la fois l'utilisation de matériel technique à des fins de vol

[447] Voir *supra* Titre 1 pour le développement sur l'utilisation des outils à des fins malveillantes, p. 37-39

[448]Le rapport abrégé rédigé par l'honorable Dianne FEINSTEIN, sénatrice américaine a été synthétisé par Eric LONDON sur le blog Mondialisation.ca, en ligne http://www.mondialisation.ca/etats-unis-le-rapport-du-senat-sur-les-interrogatoires-detaille-les-tortures-brutales-employees-par-la-cia/5419572(consulté le 12 Décembre 2014).

d'informations issues de communications, privées ou professionnelles ainsi que le vol d'informations contenues dans des bases de données logées dans des systèmes informatiques privés[449].

Cette infraction ne se retrouve pas constituée dans le cyberterrorisme lorsque l'internet est utilisé comme une cible. En effet, l'interception illégale est une étape facultative de l'activité puisque celle-ci n'en dépend pas, contrairement au cyberespionnage qui a pour finalité de récolter de l'information. Ciblé, l'internet n'est pas utilisé comme un moyen technique de commission au sens de la Convention de Budapest puisqu'il ne constitue pas en soi « un dispositif technique connecté aux lignes de transmission » ou encore, « un dispositif de collecte et d'enregistrement sans fil »[450] .

Le cyberterrorisme, qu'il soit d'origine étatique ou pas, est constitué par la commission de l'« atteinte à l'intégrité des données » encadré par l'article 4 de la convention. En son premier alinéa, celui-ci punit la corruption et la destruction des données informatiques susceptibles de causer de graves préjudices[451]. Ici, la destruction des données, tel que mentionné dans l'article, «équivaut à la destruction de biens physiques»[452].

Les cybermenaces que sont le cyberterrorisme et le cyberespionnage étatiques comportent des infractions graves, intentionnelles et sans droit[453]. A la poursuite d'une législation offrant la précision d'une définition et des composantes de ces crimes transnationaux, il

[449] Rapport explicatif, préc., note 434, p. 62.

[450] *Id*.

[451] Convention de Budapest, préc., note 46, art. 4 (1) et (2). L'article dispose ceci : « 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux. ».

[452] Rapport explicatif, préc., note 434, p. 15.

[453] « L'expression 'sans droit' tire son sens du contexte dans lequel elle est utilisée. Ainsi, sans restreindre la marge de manœuvre qu'ont les Parties pour interpréter ce concept dans leur droit interne, cette expression peut renvoyer à un comportement qui ne repose sur aucune compétence (législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle) ou à un comportement qui n'est couvert ni par des exceptions légales, excuses et faits justificatifs établis, ni par des principes de droit interne pertinents. Pour plus d'informations, voir Rapport explicatif, préc., note 428, p. 10-11

est intéressant de porter un regard sur le cadre procédural dessiné par la Convention de Budapest.

Paragraphe 2 : Le cadre procédural

Dans le texte conventionnel, ce sont les articles 14 à 21 qui consacrent les procédures utiles destinés au renforcement de « l'arsenal juridique »[454]. Ces procédures, « visent à améliorer la capacité des États à mener en temps réel leurs investigations sur les réseaux, quelle que soit la nature de l'infraction commise, et à collecter les preuves électroniques avant qu'elles ne disparaissent »[455]. Parmi elles, on note la collecte des informations ou encore le pouvoir de conserver ces informations[456]. Certaines procédures nécessitent une adoption législative au niveau des instances nationales (A) tandis que d'autres sont subordonnées à la coopération internationale entre les organes centraux étatiques (B).

A. Les instances nationales

Afin d'accélérer la collecte des indices destinés à permettre l'identification des acteurs d'une cyberopération tel que nous l'étudions, la Convention dessine deux procédures qui peuvent certainement s'y appliquer. Ce sont d'une part, l'interception de données en temps réel et d'autre part, la perquisition et la saisie des données.

L'interception en temps réel correspond à la collecte des données pendant qu'elles se créent. Elle équivaut à une mise sur écoute dans le cadre d'une enquête, opérée par les

[454]Jean François FORGERON et Virginie PRAT, « Le projet de loi portant approbation de la Convention sur la cybercriminalité », (2004) Gaz. Pal. 22, p. 3.

[455] *Id*., Université de Sorbonne, « Exposé des motifs du projet de loi relatif à la transposition de la *Convention* de Budapest en droit français », disponible en ligne : http://www.univ-paris1.fr/diplomes/master-droit-du-numerique/bibliotheque-numerique-du-droit-de-ladministration-electronique/tic/informatique/cybercriminalite/expose-des-motifs-du-projet-de-loi-relatif-a-la-transposition-de-la-*Convention*-de-budapest-en-droit-francais/ (consulté le 20 Septembre 2014).

[456] J.F. FORGERON et V. PRAT, préc., note 456, p. 3.

autorités compétentes. Les données informatiques interceptées sont davantage des métadonnées (ou « données relatives au trafic »[457]) ou des «données relatives au contenu »[458]. La procédure diffère d'un type de données à l'autre en ce que l'enquête impliquant une collecte de données relatives au trafic permet d' « effectuer des rapprochements entre l'heure, la date, la source et la destination des communications […], d'établir des liens avec les complices »[459] tandis que la prise de connaissance de la nature même de l'information (données relatives au contenu) fournira, au-delà d'indices, des renseignements plus concrets[460]. Cette procédure est très utile dans les deux cas de MSP.

[457] Les données relatives au trafic concernent toutes les informations prises à partir d'un système informatique portant sur une communication et qui peuvent être l'origine de celle-ci, sa durée ou sa date. Voir, pour plus d'informations, Convention de Budapest, préc., note 8, art 1; Rapport explicatif, préc, note 434, p. 52.

[458] Les données relatives au contenu « désignent le contenu informatif de la communication ». Pour plus d'informations, voir Rapport explicatif, préc., note 434, p. 53. Ces procédures doivent se limiter aux restrictions imposées par l'art 15 de la Convention de Budapest en étant proportionnelles à la gravité de l'infraction en cause. L'article dispose ceci :

> « 1. Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966) ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.
>
> 2. Lorsque cela est approprié eu égard à la nature du pouvoir ou de la procédure concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.
>
> 3. Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette Section sur les droits, responsabilités et intérêts légitimes des tiers.»

[459] Rapport explicatif, préc, note 434, p.53.

[460] Ce type de collecte ne devrait être autorisé que dans des cas bien déterminés car il est de nature à porter une atteinte grave à la vie privée de ou des personnes espionnés. L'ère actuelle, c'est un problème récurrent qui intervient dans l'intervention sans cesse croissante de l'État dans la régulation de l'internet. Beaucoup d'activités menées par les agences de renseignement nationales sont dénoncés à cet égard. Les nombreux partenariats qui existent entre les entreprises de télécommunications et les services de renseignements secrets sont un exemple probant de la surveillance quasi-continue qui s'exerce sur un nombre incertain de citoyens. Au Canada, l'absence de réelles informations sur les objectifs réels du partenariat entre la Sécurité Publique du Canada, la société Microsoft, Verizon et Bell Canada sème la suspicion dans le rang des défenseurs des libertés publiques. Voir R. DEIBERT, préc., note 6, p. 142 et suiv.; ou, généralement,

Mentionnons que cette procédure d'interception de données relatives au contenu existe déjà dans le *Code criminel* sous l'appellation d'« interception de communications privées»[461]. La Cour Suprême a d'ailleurs statué, dans l'affaire *R.* c. *Société TELUS Communications*, que la procédure devait être l'objet d'un mandat de perquisition spécifique distinct[462].

Zygmunt BAUMAN, Didier BIGO, Paulo ESTEVES, Elspeth GUILD, Vivienne JABRI, David LYON, and R. B. J. WALKER, « After Snowden: Rethinking the impact of surveillance », **(**2014) 8 2 *International Political Sociology* 121-144, disponible en ligne : http://search.proquest.com/docview/1559005170?accountid=12543 (consulté le 20 Septembre 2014) ; Stephen A. GRAHAM, *Surveillance and intelligence gathering in the United States: Impact and implications on privacy*, Thesis, Utica, Utica College, 2013, disponible en ligne : http://search.proquest.com/docview/1491386639?accountid=12543 (consulté le 10 Septembre 2014) ; ou, Geoffrey GORDON, « Breaking the Code: What Encryption Means for the First Amendment and Human Rights », **(**2000**)** 32 2 *Columbia Human Rights Law Review*, disponible en ligne : http://heinonline.org/HOL/Page?handle=hein.journals/colhr32&div=16&collection=journals&set_as_cursor=4&men_tab=srchresults&terms=(Prism%20program)|(eavesdrop)(america)&type=matchall (consulté le 10 Septembre 2014).

[461] Code criminel, préc., note 4, art 188. Voir aussi : la *Loi modifiant le Code criminel, la Loi sur le Service canadien du renseignement de sécurité et la Loi sur l'immigration et la protection des réfugiés*, projet de loi C-51, (dépôt et Première lecture - 30 Janvier 2015) 41ème législation (Can.); autrement appelé *Loi sur les pouvoirs d'enquêtes du 21ème siècle*, il porte sur le même type de pouvoir. Ce projet de loi vise à « apporter de nouveaux outils d'enquêtes adaptés aux délits informatiques ». Actuellement en Chambre des communes, s'il est adopté, son article 9 pourra par exemple amender l'art 342.1 (1) du code criminel :

> « 342.1 (1) Quiconque, frauduleusement et sans apparence de droit :
>
> *a*) directement ou indirectement, obtient des services d'ordinateur;
>
> *b*) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur;
>
> *c*) directement ou indirectement, utilise ou fait utiliser un ordinateur dans l'intention de commettre une infraction prévue à l'alinéa *a*) ou *b*) ou une infraction prévue à l'article 430 concernant des données ou un ordinateur;
>
> *d*) a en sa possession ou utilise un mot de passe d'ordinateur qui permettrait la perpétration des infractions prévues aux alinéas *a*), *b*) ou *c*), ou en fait le trafic ou permet à une autre personne de l'utiliser, est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable sur déclaration de culpabilité par procédure sommaire. »

L'article ne concernera donc plus uniquement le vol et la falsification des cartes de crédit. Voir en ligne Projet de loi c-51 relatif aux pouvoirs d'enquêtes du 21è siècle : http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=F&Mode=1&DocId=4745885&File=51#9 (consulté le 13 Décembre 2014) ; Il est possible de consulter l'historique de la loi en ligne : http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=F&Mode=1&billId=4740078 (consulté le 13 Décembre 2014) ; voir aussi note 253 et 279.

[462] *R.* c. *Société TELUS Communications*, [2013] 2 RCS 3, 2013 CSC 16 (CanLII), disponible en ligne : http://www.canlii.org/fr/ca/csc/doc/2013/2013csc16/2013csc16.html?searchUrlHash=AAAAAQAUbWFuZ

Distinct de l'interception des données en temps réel, le pouvoir d'enjoindre une entité à produire des renseignements permet aux organes nationaux habilités puissent obtenir une information dans le cadre d'une enquête. L'injonction de produire, consacrée par l'article 18 de la *Convention de Budapest* permet de demander à tout détenteur d'une information utile de les communiquer aux organes étatiques compétents. L'information demandée dans l'injonction doit être proportionnelle aux besoins de l'enquête. Suivant le texte, elle peut s'adresser à tout fournisseur de services ou d'accès internet en tenant strictement compte des besoins de l'enquête, en respectant une échéance soumise au respect des articles 14 et 15 de la Convention[463].

L'opinion publique et la communauté internationale ont condamné l'administration Obama pour son vaste réseau d'espionnage en exécution du programme *Prism*[464] au motif que les collectes de métadonnées étaient excessives. Ceci illustre les abus du pouvoir d'injonction car ces ordres de produire délivrées aux fournisseurs d'accès internet ont permis l'écoute de certains dirigeants européens alors même qu'elles ne s'inscrivaient pas

---

GF0IG1lc3NhZ2UgdGV4dGUAAAAAAQ (consulté le 6 Novembre 2014) ; Radiocanada.ca, « La Cour suprême exige un mandat spécifique pour les messages textes », 27 Mars 2013, disponible en ligne : http://ici.radio-canada.ca/nouvelles/National/2013/03/27/001-cour-supreme-cellulaire-saisie-jugement.shtml (consulté le 11 Décembre 2014).

[463] Les articles 14 et 15 de la Convention de Budapest sont relatifs à la protection des droits de l'Homme, au respect de la proportionnalité dans la mise en œuvre de chaque procédure et l'application de chaque pouvoir. L'article 15 vient encadrer les pouvoirs reconnus en précisant la nécessité d'une supervision judiciaire « ou d'autres formes de supervisions indépendantes » du pouvoir exécutif au plan national.

[464]Le programme Prism a été élaboré sur la base du très controversé *Patriot Act* des États-Unis adopté suite aux évènements du 9/11. Ses dispositions portent essentiellement sur un renforcement des normes et des techniques de surveillances des personnes soupçonnées d'avoir un lien quelconque avec une organisation terroriste. Pour des informations plus précises, voir The USA PATRIOT ACT: Preserving Life and Liberty, P.L. 107-56, 115 Stat. 272 **(**2001**),** disponible en ligne http://www.justice.gov/archive/ll/highlights.htm (consulté le 15 Septembre 2014). Le Canada a également adopté des mesures similaires, voir, pour plus d'informations PARLEMENT DU CANADA, Division du droit et du gouvernement, « La « Patriot Act » des États-Unis et la *Loi Antiterroriste* du Canada : Principales différences entre les deux approches législatives », Jennifer WISPINSKI, 2006, disponible en ligne http://www.parl.gc.ca/content/lop/researchpublications/prb0583-f.htm (consulté le 10 Septembre 2014). Steven GRAHAM élabore une comparaison entre les actes contre le terrorisme du Canada et des États-Unis; voir généralement Stephen A. GRAHAM, préc., note 458.

dans le cadre des enquêtes préventives de lutte contre le terrorisme[465] et n'étaient pas proportionnelles aux besoins de ces enquêtes.

L'article 18 de la Convention, fortement similaire aux dispositions américaines ayant permis l'exécution du programme *Prism*, comporte donc des limites. En effet, chaque État pourrait dès lors émettre cette mise en demeure conformément à son droit interne[466], sous réserve du respect de la proportionnalité dans la collecte des données lors d'une investigation.

Un pan de la législation internationale prend en compte le volet de la coopération internationale. Par rapport à cela, le texte conventionnel prescrit des procédures dont la mise en œuvre dépend de l'entraide internationale. Deux démarches principales requièrent la pleine coopération entre les différents organes compétents dédiés à l'entraide internationale. Ce sont la perquisition et la saisie de données d'une part, et la conservation de données, d'autre part.

B. Les organes centraux de coopération étatiques

Les organes centraux mettent en œuvre une perquisition et une saisie de données dans le cas où une aide leur est demandée de la part des autorités centrales d'un autre pays. La virtualisation du cyberespace oblige l'entraide internationale, puisque la saisie ne peut se faire qu'en copiant les données à partir du support de l'information, ou en saisissant le matériel lui-même. La procédure semble toutefois défaillante dans le cadre du cyberespionnage étatique puisque l'aide requise à un État acteur de la cyberopération risque de ne jamais avoir une réponse.

[465] Pour plus d'informations sur les différentes décisions rendues sur l'application du Patriot Act, voir Christopher P. BANKS and Steven TAUBER, « U.S. District Court Decision-Making in USA PATRIOT Act Cases after September 11 », **(**2014**)** 35 *Just. Sys. J.* 139.

[466] Convention de Budapest, préc., note 8, art. 19(1).

Toujours dans le cadre de la collaboration internationale, la procédure de conservation des données a été consacrée par l'article 16 de la Convention dans le souci de préserver l'intégrité des données qui pourraient être utiles dans une enquête. Celle-ci nécessite la mise en place de moyens informatiques destinés à la conservation de ces données. La faculté est donc laissée aux organes compétents de mettre en œuvre ou de forcer la mise en œuvre de toute conservation de données utiles[467] dans le cadre d'une enquête quelle que soit leur emplacement. La Convention de Budapest situe la période de conservation des données à un délai maximal de 90 jours renouvelable.

Pour illustrer, dans la préparation d'un acte de cyberterrorisme, l'agent mène indubitablement des recherches de plans informatiques, procède très souvent à des téléchargements de programmes malveillants, ou tout simplement communique ses intentions à ses pairs[468]. Il laisse alors des traces sur les serveurs des fournisseurs d'accès à l'internet[469]. Ce sont ces données ou métadonnées qui peuvent faire l'objet d'une demande d'injonction de conservation par l'État demandeur.

Section 2 : Le Canada dans une démarche d'uniformisation internationale

Les cyberopérations considérées comme des MSP sont des menaces pour la paix et la sécurité internationale. Elles obligent, à notre sens la communauté internationale à s'allier afin de les affronter dans un cadre légal. Pour ce faire, elle doit miser sur une forte coopération internationale (Paragraphe 1). Dans ce jeu constructif de légifération globale, l'autorité canadienne est appelé à jouer un rôle important. A la suite du premier paragraphe, nous élaborerons sur les perspectives de cette uniformisation du point de vue canadien (Paragraphe 2).

[467] La pression dans ce cas est mise sur les opérateurs et les fournisseurs d'accès de réseaux informatiques comme Google ou Yahoo.

[468] Voir *supra* comment les terroristes utilisent l'internet comme un outil de commission, p. 25-26.

[469] Pour davantage d'informations sur les cookies, voir en ligne http://www.cai.gouv.qc.ca/documents/CAI_FI_internet.pdf ou http://www.cnil.fr/vos-droits/vos-traces/ (consultés le 13 Septembre 2014).

Paragraphe 1 : La coopération internationale comme outil indispensable de prévention

La Défense est un secteur très sensible des relations internationales et appelle l'exclusive compétence nationale. Dans le cadre de la lutte contre les MSP, le Canada se place au troisième rang mondial de l'implication pour cette lutte[470]. Ainsi, le cadre légal international devra également prendre en compte cet aspect car, l'enjeu nécessite une implication conjointe de plusieurs États. A cet égard, c'est encore la Convention de Budapest qui nous indique les lignes d'une coopération efficace au plan international. En effet, elle instaure une collaboration institutionnelle sur la circulation informationnelle par les agences de renseignements (A) et une entraide conventionnelle dans la répression (B).

A. La gestion du flux informationnel par les agences internationales de renseignements

Lorsqu'un État A est victime d'une cyberinfraction, il peut, par tous moyens sécurisés, joindre un autre État B[471] sur le territoire duquel l'attaque semble provenir. En retour, l'État B peut refuser d'accéder à cette demande si son droit pénal interne ne fait pas de l'infraction un crime punissable[472]. L'article 26 de la Convention évoque la possibilité par un État de transmettre sans demande préalable de l'État destinataire des informations qu'il détient et qu'il sait pouvoir lui être utile sous conditions, s'il y a lieu.

Plusieurs États non européens ont ratifiés la Convention de Budapest[473], que ce soient des États qui, entre eux, avaient déjà des accords bilatéraux ou multilatéraux[474] ou ceux qui

[470] Benoît DUPONT, *International cooperation against cybercrime*, ICSS, Université de Montréal, 2015.

[471] Convention de Budapest, préc., note 8, art. 25 (1).

[472] *Id.*

[473] Ce sont par exemple le Canada et les États-Unis. Pour une vue plus exhaustive sur les États ayant ratifié la convention, voir *supra* note 321.

[474] C'est le cas de la coopération bilatérale existante entre les États-Unis et le Canada sur la mise en œuvre du plan d'action portant entre autres sur le renforcement de ma sécurité des infrastructures essentielles des deux pays. Cette entente fut signée le 4 Février 2011 par le Premier Ministre Stephen Harper et le Président

n'en avaient pas du tout. Dans ce cas, le texte trace un cadre général de procédure d'échange d'informations au niveau des institutions des États-membres qui doivent créer en leur sein des organes centraux dont la compétence exclusive est « d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution »[475]. Ces organes « centraux » sont d'autant plus utiles qu'ils permettent de rallier plusieurs points géographiquement éloignés avec une célérité très utile dans la lutte[476]. Les auteurs du rapport explicatif mentionnent :

> « En premier lieu, la transmission directe d'une demande entre ces autorités est plus rapide et efficace que la transmission par la voie diplomatique. Ensuite, ces autorités veillent à ce qu'il soit donné suite avec diligence aux demandes qu'elles adressent ou qu'elles reçoivent, et s'assurent que les responsables de l'application des lois dans le pays partenaire sont informés de la meilleure façon de tenir compte des règles juridiques en vigueur dans la partie requise et qu'il est donné suite comme il convient aux requêtes particulièrement urgentes ou délicates » [477].

Au Canada, advenant la ratification de la Convention de Budapest par le gouvernement fédéral, ce seront alors les principaux organes institués par le SP qui seront en relation directe avec les partenaires internationaux partis au texte. Cette procédure est pertinente puisqu'elle trace un pont de collaboration sans obliger à signer un partenariat bilatéral[478] mais les parties coopérantes sont obligées l'une envers l'autre[479].

Ce type de coopération qui existe, certes déjà au plan international, devra être compris dans tout effort de coopération internationale dans une volonté commune de règlementation des MSP. Elle permettrait par exemple de rassembler rapidement

---

américain Barack OBAMA. Voir : GOUVERNEMENT DU CANADA, *Par-delà la frontière : une vision commune de la sécurité du périmètre et de la compétitivité économique*, préc., note 288.

[475] Convention de Budapest, préc., note 8, art. 27 (2.a).

[476] Rapport explicatif, préc., note 432, p. 68.

[477] *Id*.

[478] La Convention de Budapest permet toutefois que des accords soient signés après son entrée en vigueur et que les ententes conclues priment sur le texte européen.

[479] Convention de Budapest, préc., note 8, art. 27 (c) et (d).

l'information concernant une menace informatique détectée. Elle pourrait alors être plus vite maîtrisée.

B. Les entraides conventionnelles dans la répression

Lorsqu'une attaque affecte une infrastructure numérique d'un État A, celui-ci peut requérir d'un État B d'où semble provenir l'infraction, de collecter et de conserver rapidement des données utiles aux enquêtes menées[480]. La célérité peut être exigée en demandant à l'État requis d'utiliser des moyens techniques présents sur son territoire, en prenant le soin de motiver la demande. Ainsi, si, dans le cadre de la collecte de données, il apparaît qu'une personne morale de droit privé participe à l'infraction, l'État requis doit sans délai en avertir la partie requérante[481]. Elle a toutefois la possibilité de s'opposer à cette divulgation si ses intérêts risquent d'être compromis[482].

Par ailleurs, les frontières ne permettant pas de se rendre sur les lieux soupçonnés de commission de l'infraction et d'y mener des enquêtes, la Convention institue une promptitude dans le traitement et dans l'enquête sur le territoire concerné par les autorités en place. En ce sens, l'article 31 recommande à la Partie requise de permettre à la partie requérante d'accéder aux données suite à une perquisition et une saisie[483] qu'elle aura elle-même effectuer pour la divulguer par la suite à la partie requérante. Cette divulgation est subordonnée au consentement des autorités concernées et aux particuliers, le cas échéant[484].

---

[480] *Id*., art. 29. Il est bien entendu que cette procédure ne peut aboutir que si l'État lui-même n'est pas impliqué dans l'attaque. Basé sur le principe de la bonne foi dans les relations interétatiques, la procédure s'avère cependant pertinente.

[481] *Id*., art. 30; J. F. FORGERON et V. PRAT, préc., note 456, p. 4.

[482] Convention de Budapest, préc., note 8, art. 30.

[483] *Id.,* art. 31.

[484] *Id.*, art. 32.

La Convention de Budapest érige différents principes de collaboration interétatique pour une coopération effective dans une logique de répression des cybercrimes. Elle va jusqu'à initier la création d'un contact au sein des organes centraux pour relayer en tout temps toute information dans le domaine de la cybercriminalité informatique susceptible de permettre l'avancement des mesures cybersécuritaires. C'est en ce sens que l'article 35 dispose :

> « Article 35 – Réseau 24/7
>
> 1. Chaque Partie désigne un point de contact joignable 24 heures sur 24, sept jours sur sept, afin d'assurer la fourniture d'une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes :
>
> a. apport de conseils techniques;
>
> b. conservation des données conformément aux articles 29 et 30 ; et
>
> c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.
>
> 2. a. Le point de contact d'une Partie pourra correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.
>
> b. Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités selon une procédure accélérée.
>
> 3. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau. »[485]

En définitive, le texte fournit de précieuses indications sur les procédures utiles aux enquêtes pour obtenir des éléments de preuve susceptible de contribuer à des investigations plus abouties et pertinentes à la prévention des MSP, ainsi qu'à leur répression lorsqu'il implique des acteurs non étatiques.

[485] *Id.*, art 35.

Par ailleurs, constatant que la cyberstratégie canadienne ainsi que les textes de lois actuellement en vigueur ne comportent aucun aspect légal précis de lutte contre les MSP, il importe de mettre en perspective les différentes données analysées tout au long de ce travail afin de déterminer si les différents paramètres considérées sont pertinents au plan national.

Paragraphe 2 : L'applicabilité à l'espace canadien

En dépit de sa contribution majeure à la lutte contre les MSP, le texte conventionnel ne permet de toute évidence pas la constitution d'un cadre légal de lutte contre les MSP étudiées. Elle demeure le seul texte de valeur internationale qui s'applique aux crimes informatiques et qui, nous l'avons vu, défini les grandes lignes d'une législation internationale. Cette uniformisation légale se heurte à la volonté participative des États dans la répression de crimes dont ils sont parfois partie prenante. Bien que cela n'entrave pas le premier volet de la mise sur pied d'un cadre légal global, qui fonde la qualification adéquate des MSP, cet obstacle entrave la formation de réels liens de coopération.

L'analyse de ces obstacles se fera en deux points fondamentaux. D'une part, sera abordée la problématique de la responsabilité des auteurs des cybercrimes majeurs, notamment ceux du cyberespionnage étatique (A) et, d'autre part, le voile opaque des éléments de défense intérieur sera considéré (B).

A. L'effectivité de la coopération internationale

Plusieurs auteurs affirment que la souveraineté de l'État s'érode lorsqu'elle entre dans le cadre de la coopération internationale[486]. A ce titre, ils avancent l'ingérence des organisations internationales dans la politique nationale d'un État[487].

[486] *Id.*

Dans le cas d'une coopération telle que définie par la Convention de Budapest, deux secteurs étatiques sont concernés, le secteur de la défense et le pouvoir législatif[488]. L'État canadien devrait partager ses ressources informationnelles en cas d'appel à l'entraide et devrait développer des acquis communs avec les autres États-partis. Il s'engagerait ainsi à faire part d'informations confidentielles à un autre État dans le cadre d'une enquête, à utiliser ses moyens techniques propres pour recueillir l'information requise. Il devrait entres autres, fournir à l'autre État des renseignements sur des sujets techniques relatifs à la protection à mettre en place pour une meilleure prévention des risques liés aux cybercrimes. En ce sens, le Canada partagerait ses secrets de cyberdéfense avec une autre entité étatique sans que cela soit systématiquement réciproque[489].

Ainsi, selon la Convention de Budapest, un État qui crée un organe central d'entraide[490] doit fournir tous les détails relatifs à la procédure de saisie de cette instance et, conséquemment, montrer un schéma du fonctionnement de ces instances internes. Il permet aux États, d'avoir une base d'échange d'informations, d'accéder à son réseau internet par exemple. Cela constitue également un risque pour le cas où l'institution demandeuse est infectée, d'un virus espion, qui pourrait aussitôt parasiter les fichiers demandés qu'elle transfèrera à l'État requérant.

Lorsqu'un État comme le Canada fournit également de l'information dans un domaine tel que la cybersécurité, il donne aussi aux États avec lesquels il n'est pas forcément allié des facilités pour porter atteinte à son réseau[491]. En effet, en mettant en place une stratégie de

---

[487] Jeffrey ROY, « Security, Sovereignty and Continental Interoperability: Canada's Elusive Balance », **(**2005**)** *Social Science Computer Review* 23 463-474.

[488] La vocation première de la Convention étant d'harmoniser la répression pénale des cybercrimes, le pouvoir législatif de chaque pays est concerné.

[489] Bruce SCHNEIER, Secrets and lies: digital security in a networked world, Toronto, John Wiley, 2000, p. 54-56.

[490] Convention de Budapest, préc., note 8, art 27.

[491] Ce risque est plus réel lorsqu'il s'agit d'un État qui mène une compétition économique avec le Canada. J. LEWIS, préc., note 14, p. xiii préconise donc une alliance suivant les intérêts du pays.

communication entre ces deux États, il établit un pont entre lui et cet État et partage aussi des éléments de son procédé sécuritaire d'échange cybernétique.

Il est d'ailleurs intéressant de noter la quasi-similarité des cyberstratégies de sécurité nationale entre plusieurs pays américains [492] qui, pour montrer leur engagement à renforcer la sécurité des différents secteurs critiques, ont chacun, au plan national, adopté des mesures similaires dans leur ordonnancement interne. Ceci s'explique par l'intérêt de l'État de ne pas laisser filtrer de l'information concrète sur ses installations, rendant imprécises ses publications sur le sujet[493]. En effet, pour les États, reproduire les standards de stratégie émis par les autres États leur permet de ne pas dévoiler leurs réelles intentions[494].

Au niveau du pouvoir législatif, ce sont les normes que le gouvernement canadien sera amené à adopter suivant les directives conventionnelles qui illustreront le changement effectif apporté. Ainsi, le gouvernement devra, par exemple, compléter sa loi anti-terroriste pour la pénalisation du cyberterrorisme [495] relativement aux procédures d'enquêtes[496].

Cet obstacle semble amplifié par la nécessité de conserver les affaires de l'État secrètes. Ceci étale un voile opaque sur la coopération qui ne laisse pas filtrer des informations utiles.

---

[492] B. DUPONT, « Cyber operations and the jus ad bellum revisited », préc., note 332, p. 67-80.

[493] *Id.*, p. 71.

[494] Anonymous, « Intelligent intelligence; national security », 2014, The Economist, disponible en ligne: http://search.proquest.com/docview/1546428533?accountid=12543 (consulté le 15 Octobre 2014) [Anonymous].

[495] Pour plus d'informations sur la *Loi antiterroriste* L.C. 2001, ch. 41, voir PARLEMENT DU CANADA, Division du droit et du gouvernement, « La « Patriot Act » des États-Unis et la *Loi Antiterroriste* du Canada : Principales différences entre les deux approches législatives », préc., note 466.

[496] Voir *supra*, note 256 et 282; c'est d'ailleurs en ce sens que le gouvernement canadien a introduit le projet C-51 qui est actuellement étudié en Chambre des communes.

B. Le voile du secret gouvernemental

La souveraineté[497] d'un État[498] comporte plusieurs éléments où la sécurité intérieure a une place prédominante[499]. Celle-ci implique des secrets officiels concernant les activités liées ou, ayant de quelque façon, trait à la garantie de la paix et de la sécurité nationale. Ces activités mettent en scène des institutions, des organes étatiques, des groupes de personnes ou des individus qui produisent du renseignement de sécurité[500]. Ces renseignements de sécurité, parce qu'ils constituent et servent à consolider le pouvoir de l'autorité étatique et justifient ses prérogatives ne sont pas accessibles à l'individu lambda, ou le sont dans des cas exceptionnels. Autrement dit, le renseignement de sécurité, dépendant bien sûr de sa nature est l'assise du pouvoir étatique[501] et lui conserve sa prééminence sur toutes les autres entités.

Le Canada dispose de plusieurs organes en charge de sa sécurité passive, active[502] et de la recherche continuelle d'une amélioration de son infrastructure numérique. En ce sens, il existe plusieurs organes de défense[503] qui assurent une protection continue au pays en respect aux normes encadrant leurs activités[504]. Les renseignements de sécurité produit par ces agences peuvent être relatives à la recherche sur de nouvelles armes, sur de

[497] Pour Ken ROACH, *September 11: Consequences for Canada* , 1st, Montréal, Mc Gill Queen's press university, 2003, p 133 et suivants, la souveraineté canadienne est comparable à une pièce de pâtisserie que les autres puissances essaient de se partager. Elle effectue une étude très instructive des conséquences du drame du 11 Septembre sur le Canada ; disponible en ligne : http://site.ebrary.com/lib/umontreal/docDetail.action?docID=10119840&token=c59682f0-b81b-4b83-9ea2-673101aef99f(consulté le 3 Septembre 2014).

[498]La Charte, préc., note 325, art 2 (1).

[499]Voir *supra*, p. 49-57 où sont définis plus précisément les différents organes et les textes se rapportant à la sécurité intérieure du Canada.

[500]*Id*.

[501] La confidentialité des activités des agences de renseignements est une condition d'exercice de la souveraineté nationale s'inscrivant dans ses compétences nationales. Serge SUR, « La souveraineté internationale », (2012) 363 *Recueil des cours* 89.

[502] J. LEWIS, préc., note 14, p. 90-94.

[503] Voir *supra*, p. 49-57.

[504]*Id.*

nouveaux programmes de défense, sur de la recherche scientifique[505]. Ces activités peuvent également porter sur l'élaboration de nouvelles armes ou de nouveaux systèmes de défense, de nouvelles logistiques de surveillance, de nouveaux procédés de prévention[506].

La nécessaire confidentialité ici peut être appréciée, d'une part, comme une obligation sociale[507] destinée à préserver l'ordre interne et, d'autre part, comme l'expression d'un souci de protection de la propriété intellectuelle. La confidentialité des secrets officiels vue comme une obligation de préservation de l'ordre sociale interne peut être analysée de façon empirique. Aussi est-il intéressant de porter un regard sur le panorama factuel qui a résulté du dévoilement des surveillances qu'opéraient les États-Unis dans le cadre de son programme de défense nationale ou encore les révélations de Julian Assange par les fameux Wikileaks[508]. A l'instar de ces exemples qui ont causé des protestations sociales, le cas de l'étude menée par Human Right Watch[509] exposant les pratiques des services de renseignements américains qui avaient leur part à jouer dans l'élan terroriste[510] est très actuel. Toujours dans le cadre de l'obligation sociale, une activité officielle peut porter sur

[505] Anonymous, préc., note 496.

[506] *Id.*

[507] Nicolas VERMEYS, « Cadre législatif de l'obligation de sécurité – Responsabilité pénale », **(**25 Février 2014**)**, Cours n°8, DRT 6929M.

[508] Voir le dossier constitué en ligne http://www.liberation.fr/wikileaks-revelations-en-serie,99982 (consulté le 19 Août 2014).

[509] HUMAN RIGHT WATCH, « États-Unis : Les poursuites judiciaires liées au terrorisme sont souvent basées sur des motifs illusoires », disponible en ligne http://www.hrw.org/fr/news/2014/07/21/État s-unis-les-poursuites-judiciaires-liees-au-terrorisme-sont-souvent-basees-sur-de (consulté le 4 Septembre 2014).

[510] Alex PANETTA, « Les autorités américaines créent des terroristes, selon une étude », 21 Juillet 2014, disponible en ligne : http://www.lactualite.com/actualites/monde/les-autorites-americaines-creent-des-terroristes-selon-une-etude/ouhttp://www.985fm.ca/national/nouvelles/les-autorites-americaines-creent-des-terroristes-332626.html(consulté le 16 Août 2014) ; « Le FBI a poussé des Américains musulmans à commettre des attentats », en ligne :http://www.ledevoir.com/international/État s-unis/414010/État s-unis-le-fbi-a-pousse-des-americains-musulmans-a-commettre-des-attentatsou encore cet exemple empirique de la méthode de « création » des terroristes par le FBI, disponible en ligne :http://www.lapresse.ca/international/États-unis/201407/21/01-4785493-comment-le-fbi-aurait-cree-des-terroristes.php (consulté le 15 Août 2014).

une enquête en cours[511], dont la divulgation pourrait porter préjudice au bon achèvement de l'investigation.

Il en découle que les activités des services de renseignements canadiens représentent des secrets dont ils ne peuvent se départir. En l'exposant dans le cadre de la coopération internationale, les agences canadiennes courent des risques certains.

En définitive, le second volet relatif aux mécanismes de coopération internationale couvert par la Convention de Budapest que nous mettions en avant dans notre énoncé ne semble pas rencontrer des critères empiriques favorables à un échange international productif. Ce constat porte sur deux raisons essentielles à savoir l'implication des États dans les cybercrimes objets de la coopération compris dans les affaires de sécurité intérieure et, le secret gouvernemental.

[511]Serge SUR, préc., note 504, p. 7-14.

Conclusion

Le gouvernement canadien a conscience de la vulnérabilité de ses infrastructures physiques et numériques face aux MSP. Cela s'illustre par la publication de la cyberstratégie canadienne qui contient des mesures ambitieuses[512], dont les avancées témoignent de leur utilité et de la ferme volonté gouvernementale, notamment du SP, de freiner la montée de ces menaces. Au plan législatif, dans l'éventuelle perspective de ratification de la Convention de Budapest, le pays a introduit le projet C-51 qui autorise de nouveaux pouvoirs d'enquête adaptés aux cybercrimes.

Les autorités fédérales ont, également, conclu plusieurs alliances avec des gouvernements étrangers, afin de participer activement à la dynamique internationale de lutte contre le cybercrime en général. Sur cette lancée, le pays se retrouve à la 3ème place dans un classement effectué par Benoit Dupont sur les différents pays ayant le plus de visibilité sur le plan international dans la lutte contre le cybercrime. Il fait donc partie du peloton de tête de la lutte devant ses alliés du FVEY.

Toutefois, comme nous l'avons vu, le gouvernement canadien n'a pas pu empêcher le cyberespionnage dirigé contre Ottawa[513], le piratage de la plateforme internet de Terrasse Vaudreuil[514] ou encore, les nombreux départs de canadiens pour le djihad grâce au prosélytisme opéré par les cyberterroristes[515]. Est-il possible que l'adoption du projet de loi C-51 puisse aider à empêcher ou prévenir une cyberattaque comme celle menée contre

[512] Les experts ayant collaboré avec le SDA affirment que la cyberstratégie canadienne est un ensemble de mesures amitieuses. SDA, préc., note 9, p. 74.

[513] Voir note 30.

[514] En 2015, par exemple, des terroristes se réclamant du Groupe État Islamique ont exploité les failles de sécurité de plusieurs sites français et de la plateforme de la municipalité de Terrasse-Vaudreuil. Les islamistes du mouvement Mile East Army ont revendiqué le détournement de la plate-forme de la municipalité pour y faire leur propagande. Voir en ligne : ici.radio-canada.ca/audio-video/media/2015/01/23/Le-site-Internet-de-Terrasse-Vaudreuil-pirate?externalId=7233048&appCode=medianet (consulté le 23 Janvier 2015).

[515] Rdi.ca, « De jeunes Québécois soupçonnés d'avoir rejoint des djihadistes en Syrie », disponible en ligne : http://ici.radio-canada.ca/nouvelles/societe/2015/02/25/006-jeunes-quebecois-quitte-pays-syrie-djihadistes.shtml (consulté le 10 février 2015).

la chaîne de télévision française TV5[516]? En définitive, faut-il uniquement se préoccuper de la légifération de la cybercriminalité de type 2?

Ainsi, en dépit des nombreux efforts déployés par le ministre du SP et le gouvernement canadien en général[517], le Canada est encore critiqué pour son action très lente dans la mise en marche d'une cybersécurité collective[518].

Vu la gravité des effets qu'une MSP peut entraîner[519], il importe d'envisager une adoption de règles adéquates identifiant juridiquement ces cybermenaces afin qu'une réelle défense puisse être efficace. Nous le mentionnions dans l'introduction, les normes internationales représentent un apport considérable au renforcement de la cybersécurité canadienne. Ce renforcement doit se faire à deux niveaux.

Le premier niveau porte sur le volet international de la cybersécurité. La manœuvre d'une cyberattaque de type 1 implique plusieurs juridictions à cause de l'ubiquité de cet environnement numérique. Considérant donc qu'il s'agit d'un espace international, nous avions cherché à identifier juridiquement les MSP sans arriver à une qualification claire. Au vu des différents concepts existants dans le droit international régissant les relations entre États, nous en sommes arrivés à la conclusion que les cyberattaques de type 1 auquel un État a participé de façon directe ou indirecte était globalement un acte international illicite. L'absence de réponse précise à ces problématiques s'explique en général par l'inexistence au plan international de textes ayant une valeur légal spécifique à l'espèce. En ce sens, M. Castle affirme:

> « Preventing and stopping a cyber attack, especially against the critical infrastructures of a particular state, requires the co-operation and assistance of all states in the investigation of such attack and in blocking all traffic

[516] Voir notes 24,80 et 132.

[517] En effet, suivant l'évaluation effectuée par le SDA, le pays obtient un score de 3 ½ étoiles derrière le Danemark, l'Estonie, la Finlande, les Etats-Unis, la France et l'Angleterre. SDA, préc., note 9, p. 74-85.

[518] *Id*.

[519] Isaac Ben-Israel affirme: «If you want to hit a country severely you hit its power and water supplies. Cyber technology can do this without shooting a single bullet ». SDA, préc., note 9, p. 7.

> with the offending state Internet Service Providers. Multilateral responses are necessary as they are in other situations involving threats to international peace and security. Cyber attacks are a global problem like global warming, because no one state can deal adequately with the problem on its own. Existing customary and conventional international law rules are not as clear and effective when applied to a cyber attack by an organ or agent of a state or by its sponsored terrorist organizations as when applied to a cyber attack by a non-state actor. Simply reaffirming the applicability of present international law rules to cyber attacks is not sufficient. »[520] [Nous soulignons]

Bien que les règles du *jus ad bellum* ne définissent pas clairement le régime juridique des cyberattaques de type 1 lancés par des États ou leurs émissaires, elles apportent des indications sur le raisonnement à mener et suivant le Manuel de Tallinn, ces règles de droit international peuvent s'appliquer dès lors que les dommages causés sont aussi dévastateurs que ce qu'engendrerait un usage illégal de la force. Cependant, cette théorie est très aléatoire puisqu'elle exclue une bonne partie des types de manifestations des cyberattaques majeures actuelles. De ce point de vue, la Convention de Budapest semble apporter plus d'indications sur la nature juridique que pourrait revêtir au plan international, les MSP.

Il importe alors que le gouvernement canadien établissent ou élargissent ses partenariats en matière de cybersécurité à l'échelle planétaire. Une première étape essentielle dans cette logique serait la ratification du texte conventionnel. Advenant que la ratification ne soit pas effective, le gouvernement pourrait envisager de rédiger un projet de loi qui définirait clairement les natures juridiques des MSP et donc leur régime juridique au plan national, à défaut. Néanmoins, cela ne résoudrait pas le problème que pose l'ubiquité du cyberespace. C'est à cette fin qu'au niveau international, ces précisions législatives devraient être faites. Elles permettraient ainsi à tous les pays connectés d'avoir des bases communes pour l'identification des cybercrimes de type 1[521].

[520] M. CASTLE, préc., note 35, p. 15.

[521] J. LEWIS, préc., note 14, p. 69.

Toujours au plan international, mais dans une perspective de coopération internationale[522], il serait intéressant qu'avec les autres membres des FVEY, le gouvernement canadien initie et encourage une ouverture des centres de gestion d'urgence des incidents cybernétiques aux autres pays non alliés afin d'amorcer une coopération internationale productive. Il ne s'agit pas, dans notre entendement de construire une coopération internationale dans le but de publier une cyberstratégie internationale commune à tous les États interconnectés ou non. Rafal Rohozinski répond d'ailleurs : « […] afin de lutter contre la cybercriminalité, il faudrait conclure un accord mondial, ce qui est très peu probable actuellement » au Comité permanent sur la défense nationale lors de sa présentation préliminaire sur l'état actuel de la cybersécurité canadienne[523].

Bien que nous affirmions que la coopération internationale est un élément essentiel du renforcement de la cybersécurité nationale, il est essentiel de considérer que les États n'ont pas tous des intérêts convergents qu'ils soient alliés ou non. Ce blocage majeur exige donc une tempérance dans la conclusion des éventuels futurs partenariats. Il est suivi de la définition très aléatoire de la vie privée des citoyens variant d'un pays à l'autre [524] . C'est aussi ce qui explique le refus de poursuivre l'adoption d'une cybersécurité globale voulu par de plusieurs auteurs. Ainsi, une cybersécurité globale « idéale » à l'image de ce que décrit Seymour Goodman, qui comprendrait l'harmonisation des capacités cybersécuritaires communes[525] semble un vœu pieux[526].

[522] SDA, préc., note 9, p. 18. Plusieurs experts en cybersécurité encouragent une solide coopération internationale dans le domaine' en ce sens, Vytautas Butrimas, le conseiller en chef de la cybersécurité près le Ministère de la Défense de la Lithuanie affirme : « There are holes in the systems. We need to reduce the risk of another state placing something as a logic bomb that would cause system to shut down. There is no such thing as zero risk but we can make the risk acceptable ». Il rappelle l'urgence d'une coopération internationale à l'ère où les MSP prennent de l'ampleur.

[523] CHAMBRE DES COMMUNES DU CANADA, préc., note 312, p. 2.

[524] SDA, préc., note 9, p. 24.

[525] J. LEWIS, préc., note 14, p. 71.

[526] Hamadoun Touré, secrétaire général de l'Union internationale des télécommunications en 2010, affirmait que les Nations-Unies devraient adopter un « cybertraité de paix ». Cette volonté semble être une utopie à l'heure actuelle. Voir SDA, préc., note 9, p. 26.

En définitive, nous pensons que la communauté internationale devrait porter ses réflexions sur l'élaboration d'une ensemble normatif qui ciblerait uniquement les cybercrimes de type 1 en précisant leur nature et leur régime juridique[527]. Ceci servirait alors de base à chaque État pour définir les différents éléments de leurs défenses passive et active. L'enjeu étant planétaire, le gouvernement canadien ciblerait alors les États avec lesquels il est allié pour établir des partenariats fondés sur des codes de conduite[528], sur un échange d'informations continu dont un organe central aurait la charge[529], tel que suggéré par la Convention de Budapest. Afin que ces partenariats soient productifs, suivant Steve Purser, il serait intéressant de mettre en place des normes techniques de cybersécurité communes comme les normes ISO[530]. Ceci confèrerait plus de crédibilités à l'État, un marché économique plus élargi, de même qu'un commerce international plus productif et moins à risque[531]. La rigueur de ses standards permettra la mise en place de systèmes de sécurité qui, même s'ils n'arrivent pas éliminer le risque, permettrait d'amortir les pertes économiques[532].

La seconde phase de renforcement de la cybersécurité nationale se déroule à la même échelle. Il est de notre avis que le gouvernement devrait dans un premier temps, ratifier la Convention de Budapest. Ensuite, un budget conséquent devrait être mis en place pour améliorer la cyberdéfense et atténuer les vulnérabilités des infrastructures critiques.

En définitive, il est certes impossible d'éliminer toutes les cybermenaces majeures comme les MSP puisque l'internet est en perpétuel mouvement mais il est crucial que son

---

[527] En ce sens, Jamie Shea soulève des questions très importantes auxquelles pourraient répondre l'ensemble normatif voulu dans ce mémoire : « How to define pre-emptive cyber-attacks? What are they? How to come up with the evidence? How strong the retaliation be? What is proportionate ? ». SDA, préc., note 9, p. 21; voir aussi Michael N. SCHMITT, « Cyber operations and the jus ad bellum revisited », préc., note 332, p. 234-243.

[528] SDA, préc., note 9, à la p. 21, selon Florian Walther, la problématique en jeu requiert un code. Il affirme : « the code defined what it could do and what polices force could do […] ».

[529] Mohd Noor Amin, dans SDA, préc., note 9, p. 24.

[530] SDA, préc., note 9, p. 23.

[531] *Id*.

[532] *Id*.

importance soit au cœur des discussions nationale et internationale. Comme l'affirme bien Rafal Rohozinski :

> « Le problème en ce qui concerne la cybersécurité, c'est que ce n'est pas aussi facile à comprendre que les soins de santé, le chômage ou d'autres enjeux sur lesquels l'électeur moyen a une opinion ou non. La cybersécurité a tendance à être un sujet beaucoup plus abstrait, ce qui signifie qu'il faut vraiment qu'il se passe un événement majeur pour qu'elle se retrouve à l'ordre du jour national, qu'on y accorde des ressources adéquates et qu'on assure le niveau de coordination nécessaire […] »[533]. [Nous soulignons]

[533] CHAMBRES DES COMMUNES DU CANADA, préc., note 312, p. 6.

TABLES BIBLIOGRAPHIQUES

Table de la législation

Textes canadiens

Projets

Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques, projet de loi, C-12, dépôt et 1ère lecture, 1ère sess., 41e légis., (Can.)

Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques (pouvoirs de rendre des ordonnances), projet de loi, C-475, dépôt et 1ère lecture, 1ère sess., 41e légis., (Can.)

Loi édictant la Loi sur la communication d'information ayant trait à la sécurité du Canada et la Loi sur la sûreté des déplacements aériens, modifiant le Code criminel, la Loi sur le Service canadien du renseignement de sécurité et la Loi sur l'immigration et la protection des réfugiés, projet de loi, C-51, dépôt et 1ère lecture, 2ème sess., 41e légis., (Can.)

Lois

Charte canadienne des droits et libertés, partie I de la *Loi constitutionnelle de 1982*, annexe B de la *Loi de 1982 sur le Canada*], 1982, c.11 (R.-U.)
Loi sur le service canadien du renseignement de sécurité, LRC 1985, c C-23.
Loi sur la protection des renseignements personnels, LRC 1985, c P-21.
Loi sur la Gendarmerie royale du Canada, LRC 1985, c R-10.
Loi sur le service canadien du renseignement de sécurité, LRC 1985, c C-23.
Loi sur la protection de l'information, LRC 1985, c O-5.
Loi antiterroriste, L.C. 2001, ch. 41

Codes

Code criminel L.R.C. (1985), ch. C-46.

Textes internationaux et régionaux

Charte des Nations Unies, **(**26 Juin 1945**)** C.N.U.O.I., vol. 15, [1945] R.T. Can n°7.

COMITÉ EUROPÉEN POUR LES PROBLÈMES CRIMINELS (CDPC), *Recommendation No. R. (95) 13*, disponible à l'adresse: http://www.coe.int/ta/rec/l995/95r13htm (consulté le 16 Septembre 2014).

COMMISSION DES COMMUNAUTES EUROPEENNES, *Livre vert sur un programme européen de protection des infrastructures critiques*, 1ère éd., COM 576 final, 2005.

COMMISSION DU DROIT INTERNATIONAL, *Projet d'articles sur la responsabilité des organisations internationales et commentaires y relatifs*, session A/66/10 **(**2011**)**, disponible à l'adresse : http://legal.un.org/ilc/texts/instruments/francais/commentaires/9_11_2011_francais.pdf (consulté le 7 Octobre 2014).

CONSEIL DE L'EUROPE, *Convention sur la cybercriminalité*- STE no. 185 **(**23 Novembre 2001**)**.

CONSEIL DE L'EUROPE, *Recommandation N° R (89) 9* (adoptée par le Comité des Ministres le 13 septembre 1989), disponible à l'adresse : https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900321&SecMode=1&DocId=702360&Usage=2(consulté le 13 Août 2014)

Projet d'articles sur la responsabilité de l'état pour fait internationalement illicite, UN Doc. A/56/10; GAOR, 56th Sess., Supp. No. 10 (2001).

Résolution 2625, UNGA Res 2625 (XXV) UN GAOR 25th Sess, Supp No 28 at 121. UN Doc A/8028 (1971).

Résolution 3314 (XXIX) de l'assemblée générale des Nations Unies UNGA Res 3314 (XXIX).

Table de la jurisprudence

Jurisprudence canadienne

Ruby c. *Canada* (Solliciteur Général), [1996] 3 CF 134, disponible à l'adresse : http://www.canlii.org/fr/ca/cfpi/doc/1996/1996canlii4052/1996canlii4052.html (consulté le 2 Avril 2014)

R. v. *Delisle*, 2012 NSPC 114

R. c. *Société TELUS Communications*, [2013] 2 RCS 3, 2013 CSC 16 (CanLII), disponible à l'adresse : http://www.canlii.org/fr/ca/csc/doc/2013/2013csc16/2013csc16.html?searchUrlHash=AAAAAQAUbWFuZGF0IG1lc3NhZ2UgdGV4dGUAAAAAAQ (consulté le 16 Septembre 2014)

Jurisprudence internationale

Activités militaires et paramilitaires au Nicaragua et contre celui-ci (*Nicaragua* c. *États-Unis d'Amérique*), compétence et recevabilité, arrêt, C. I.J. Recueil 1984

Procureur c. *Dusko Tadic* IT-94-1-A, (1999), 38 ILM.

Détroit de Corfu Royaume-Uni contre *Albanie*, [1949] ICJ Rep 4 para. 22.

France v. *Turkie* 1927 PCIJ (Ser A) No 10 para. 88.

Table de la doctrine

Monographies et ouvrages collectifs

BENYEKLEFF, K. et N. VERMEYS (dir.), *Le droit à la sécurité la sécurité par le droit*, Montréal, Éditions Thémis, 2010.

BETTATI, M., *Le Terrorisme les voies de la coopération internationale*, Paris, Odile Jacob, 2013.

BILLER, J. T., *Cyber-Terrorism: Finding a Common Starting Point*, Thesis, Faculty of the George Washington University Law School, 2012.

BLANK, A. G., *TCP/IP Jump Start: Internet Protocol Basics*, 2ème éd., Vancouver, Sybex, 2002.

CARR, J., *Inside Cyber warfare*, 2e éd, Sebastopol, O'Reilly, 2011.

CORNU Gérard (dir.), Vocabulaire juridique, 8ème, Paris, Association Henri Capitant, P.U.F., 2007.

DAVID, C.-P. et B. GAGNON (dir.), *Repenser le terrorisme Concepts, acteurs et réponses*, Québec, Les Presses de l'Université Laval, 2007.

DENNING, D., *Cyberterrorism*, USA, Nova Science Publishers Inc, 2007

DEIBERT, R. J., *Black Code Inside the battle for cyberspace*, Toronto, McClelland & Stewart, 2013

DINSTEIN, Y., *War, aggression and self-defense*, Cambridge, Cambridge University press, 2005.

GLEYZE, J.-F., *La vulnérabilité structurelle des réseaux de transport dans un contexte de risques*, Thèse de doctorat, Paris VII, Université Denis Diderot, 2002

GRAHAM, S. A., *Surveillance and intelligence gathering in the United States: Impact and implications on privacy*, Thesis, Utica, Utica College, 2013.

HOLT, T. J., *Crime-on-line correlates causes, and context*, 2nde ed., North Carolina, Carolina Academic Press, 2013.

KERSCHICHNIG, G., *Cyberthreats and international law*, Hague, Eleven International Publishing, 2012.

KRUTZ, R. L., *Securing SCADA systems*, Indianapolis, John Wiley & Sons, 2006.

LEWIS, J. (dir.), *Cyber security Turning National solutions into international cooperation*, Washington, the CSIS Press, Significant issues series, 2003.

LESSIG, L., *Code*, New York, Basic Books, 1999.

MITJANS, E. et K. BENYEKLEFF, *Circulation internationale de l'information et sécurité*, Montréal, Éditions Thémis, 2013.

MITNICK, K. D. and W. L. SIMON, *The art of deception: controlling the human element of security*, Indianapolis, Wiley, 2002.

PETIT, F., *Concepts d'analyse de la vulnérabilité des infrastructures essentielles -prise en compte de la cybernétique*, Thèse, École polytechnique de Montréal, Montréal, 2009.

ROACH, K., *September 11: Consequences for Canada,* Montréal, McGill Queen's press university, 2003.

SCHMITT, M. (dir.), *Tallinn manual on the international law applicable to cyber warfare*, New York, Cambridge Press, 2013.

SAMUEL, A. W., *Hacktivism and the future of political participation*, Thesis, Harvard's university, Cambridge, 2005.

SCHNEIER, B., *Secrets and lies: digital security in a networked world*, Toronto, John Wiley, 2000.

SCHNEIER, B., *Schneier on security*, Indianapolis, Wiley Pub, 2008.

VERMEYS, N., *Virus informatiques : responsables et responsabilité,* Montréal, Éditions Thémis, 2003.

WILSON, C., *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service Report (RL 32114)

Articles de revue et étude d'ouvrages collectifs

ANONYMOUS, « Intelligent intelligence; national security » **(**2014**)** *The Economist*.

BANKS, C. P. and S. TAUBER, « U.S. District Court Decision-Making in USA PATRIOT Act Cases after September 11 », **(**2014**)** 35 *Just. Sys. J.* 139.

BAUMAN Z., D. BIGO, P. ESTEVES, E. GUILD, V. JABRI, D. LYON, and R. B. J. WALKER, « After Snowden: Rethinking the impact of surveillance », **(**2014) 8 2 *International Political Sociology* 121.

BLANK, L. K., « International Law and Cyber Threats from Non-State Actors » **(**2013**)** 89 *Int'l L. Stud. Ser. US Naval War Col.* 415.

BRENNER S. W. and M. D. GOODMAN « In defense of cyberterrorism: an argument for anticipating cyber-attacks », **(**2002**)** 1 *U. Ill. J.L. Tech. & Pol'y*.

BRITZ, M. T., « The internet as a tool for terrorists: implications for physical and virtual worlds », in HOLT, T. J., *Crime-on-line correlates, causes, and context*, 2nde ed., North Carolina, Carolina Academic Press, 2013.

BURGER, D., « Networking the world's crime fighters», **(**18 Juillet 1996**)**, 22 *Computing Canada* 15.

CARDENAS, A. A., T. ROOSTA et al., « Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems», **(**2009**)**.

CASSIM, F., « Addressing the spectre of cyber terrorism: a comparative perspective », **(**2012**)**, 15 *Potchefstroom Elec. L.J.* 380.

CASTEL, M. E., « International and Canadian Law Rules Applicable to Cyber Attacks by State and Non-State Actors » **(**Juin 2012**)** 10 *Can. J. L. & Tech.* 89 6.

CLAUSEN, C., « Little brother is watching you » **(**Fall 2013**)** *Queen's Quarterly*.

COHEN, A., « Are we legally ready », **(**2010**)** 9 *J. Int'l Bus.& L.*1.

COLLIN, B. C., « The Future of CyberTerrorism: Where the Physical and virtual worlds converge», **(**Mars 1997**)** 13 *Crime and Justice International* 2, disponible à l'adresse: http://www.cjcenter.org/cjcenter/publications/cji/ (consulté le 10 Avril 2014).

D'ELIA, D., « La guerre économique à l'ère du cyberespace », **(**2014**)** 1-2 *Hérodote* 240.

DEIBERT, R. and N. ARELLANO, « U of T researchers uncover spy network», **(**2009**)** 25 *Computer World Canada* 7.

DETERMANN, L. et K. T. GUTTENBERG, «On War and Peace in Cyberspace- Security, Privacy, Jurisdiction », **(**2013-2014**)** 41 *Hastings Const. L.Q*. 875.

DUPONT, B., « Pourquoi les mégadonnées et la surveillance généralisée ne nous protègeront pas contre le terrorisme », **(**28 Mars 2015**)**.

DUPONT, B., L'environnement de la cybersécurité à l'horizon 2022 Tendances, moteurs et implications, Note de recherche no. 14, Montréal, 2012

FARWELL, J. P. and R. ROHOZINSKI, « Stuxnet and the Future of Cyber War », **(**February-March 2011**)** 53 *Survival* 1.

FORGERON, J.-F. et V. PRAT, « Le projet de loi portant approbation de la Convention sur la cybercriminalité », **(**2004**)** *Gaz. Pal.* 22.

GABLE, K., « Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent », **(**2010**)** 43 *Vand. J. Transnat'l L.* 57.

GALLAND, J.-P., « Critique de la notion d'infrastructure critique », **(**2010**)** 3 *Flux* 81 6.

GIACOMELLO, G., « Bangs for the buck: A cost-benefit analysis of cyberterrorism», **(**2004**)** 275 *Studies in Conflict & Terrorism* 387.

GORDON, G., « Breaking the Code: What Encryption Means for the First Amendment and Human Rights », **(**2000**)** 32 2 *Columbia Human Rights Law Review*.

IQBAL, M., « Defining Cyberterrorism », **(**2003-2004**)** 22 J. *Marshall J. Computer & Info. L.* 397.

JAGATIC, T. N., N. A. JOHNSON et al., « Social Phishing », **(**2007**)** 50 *Communications of the ACM* 10.

KERR, O. S., « U. S. dept. of justice, searching and seizing computers and obtaining electronic evidence in criminal investigations », **(**2001**)**.

KEYSER, M., « The council of Europe convention on cybercrime », **(**2002-2003**)**, 12 *J. Transnat'l L. & Pol'y* 296.

KLEIN, P., « Le droit international à l'épreuve du terrorisme », **(**2006**)** 321 *Recueil des cours* 203.

KREKEL, B., « Capability of the People's Republic of China to conduct cyberwarfare and computer network exploitation », **(**2009**)** *US-China Economic and Security Review Commission*.

LENTZ, C. E., « A State's Duty to Prevent and Respond to Cyberterrorist Acts », **(**2009-2010**)** 10 *Chi. J. Int'l L.* 799.

MILLER, R. A. and I. LACHOW, « Strategic fragility: Infrastructure Protection and National security in the information age », **(**Janvier 2008**)** 2 *Defense horizons* 59.

PLATT, V., « Still the fire-proof house? An analysis of Canada's cyber security strategy », **(**Winter 2011-12**)** *International Journal*.

POLLIT, M., « Cyberterrorism –Fact or fancy ? »

RAGHAVAN, T. M., « In fear of cyberterrorism: an analysis of the Congressional response», **(**2003**)** *U. Ill. J.L. Tech. & Pol'y* 297.

REGE, A., « Industrial control systems and cybercrime », dans HOLT, T. J., *Crime on-line correlates, causes, and context*, 2nde ed., California , Carolina Academic Press, 2013.

ROY, J., « Security, Sovereignty and Continental Interoperability: Canada's Elusive Balance», **(**2005**)**, *Social Science Computer Review* 23 46.

SCHMITT, M. N., « Cyber operations and the jus ad bellum revisited » **(**2011-2012**)** 56 *Vill. L. Rev.* 569.

SCHREIER, F., « On Cyberwarfare », **(**2015**)** *DCAF Horizon Working Paper*.

SMITH, A. M. et N. Y. TOPPEL, « Case Study: Using Security Awareness to Combat the Advanced Persistent Threat », **(**2009**)**, 13th Colloquium for Information Systems Security Education.

SPRINGER, S., H. CHI et al, « Leaky geopolitics: The ruptures and transgressions of WikiLeaks », **(**July 2012**)** 3 *Geopolitics* 07.

SUR, S., « La souveraineté internationale », **(**2012**)** 363 *Recueil des cours* 89.

TOMUSCHAT, C., « On the possible « added value » of a comprehensive Convention on Terrorism », **(**2005**)** 26 *Human Rights Law Journal*.

TRUDEL, P., « Quel droit et quelle régulation dans le cyberespace? », XXXII-2 *Sociologie et sociétés*.

VENTRE, D., « Une analyse du rapport Mandiant », **(**Juillet 2013**)**, Chaire de cyberdéfense et de cybersécurité.

VERMEYS, N., « Cadre législatif de l'obligation de sécurité – Responsabilité pénale », **(**25 Février 2014**),** Cours n°8, DRT 6929M

VILLENEUVE, N., « The "Kneber" Botnet, Spear Phishing Attacks and Crimeware », **(**2010**)**.

WEBER, A., « The council of Europe's convention on Cybercrime », **(**2003**)** 18 *Berkeley Tech. L.J.* 425.

WEIMANN, G., « www.terror.net. How Modern Terrorism Uses the Internet », **(**2006**)** Special Report, United States Institute of Peace Press.

WEIMANN, G., « Terror on the internet: the new arena, the new challenges», **(**2006**)** 4 10 *Middle East Journal* 60.

WEISBORD, N., « Conceptualizing aggression », **(**2009-2010**)** 20 *Duke J. Comp. & Int'l L.* 1 6.

WILSON, C., « Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues », **(**2008**)**, *Cong. Research Serv*.

ZIVOT, L. J., « The Transnational Dimension of Cyber Crime and Terrorism », **(**2001-2002**)** 34 *N.Y.U Journal of International Law and Politics* 475.

ZORZ, Z., « The escalating cost of US cybersecurity plans » **(**15 Février 2012**)** *Help Net security*.

Documents gouvernementaux

Documents canadiens

AFFAIRES ETRANGERES ET DEVELOPPEMENT CANADA, Canada et l'Organisation des Etats-Américains, disponible à l'adresse : http://www.international.gc.ca/american_states-etats_americains/oas-oea/oas-oae.aspx?lang=fra (consulté le 10 mai 2014).

CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS, *Rapport ITSB-65*, Juillet 2013, disponible à l'adresse : https://www.cse-cst.gc.ca/fr/node/234/html/9892 (consulté le 6 Octobre 2014)

DIVISION DES AFFAIRES JURIDIQUES ET LÉGISLATIVES, *Résumé législatif du projet de loi C-12 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques*, 19 octobre 2011.

GENDARMERIE ROYALE DU CANADA, Rapport ministériel sur le rendement, 2011-2012.

GOUVERNEMENT DU CANADA, *La GRC et la sécurité nationale du Canada*, Sa Majesté la Reine du Chef du Canada, 2011.

GOUVERNEMENT DU CANADA, BUREAU DU CONSEIL PRIVÉ, *Protéger une société ouverte: la politique canadienne de sécurité nationale*, 2004, disponible à l'adresse : http://www.bcp.gc.ca/docs/information/publications/aarchives/natsec-secnat/natsec-secnat-fra.pdf (consulté le 12 Mars 2014).

GOUVERNEMENT DU CANADA, *Étude hors-série: questions prioritaires Évaluation des cybermenaces pesant contre les infrastructures du Canada*, 2012, disponible à l'adresse : https://www.csis-scrs.gc.ca/pblctns/cdmctrch/20121001_ccsnlpprs-fra.asp (consulté le 17 Février 2014).

GOUVERNEMENT DU CANADA, *Renforcer la résilience face au terrorisme : stratégie antiterroriste du Canada*, 2013, disponible à l'adresse : http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-fra.aspx (consulté le 15 Mars 2014).

GOUVERNEMENT DU CANADA, *Par-delà la frontière : une vision commune de la sécurité du périmètre et de la compétitivité économique*, 2011.

GOUVERNEMENT DU CANADA, *Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada*, 2013.

GOUVERNEMENT DU CANADA, *Les Transports au Canada 2012*, Canada, 2013.

GOUVERNEMENT DU CANADA, *Les Transports au Canada 2013*, Canada, 2014.

GOUVERNEMENT DU CANADA, *Par-delà la frontière : une vision commune de la sécurité du périmètre et de la compétitivité économique* (2011), disponible en ligne http://plandaction.gc.ca/fr/content/dela-la-frontiere (consulté le 7 Juillet 2014).

MINISTERE DE L'INDUSTRIE, *Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police*, Centre canadien de la statistique juridique, N° 85-558-XIF, Ottawa, 2002.

MINISTÈRE DE LA SÉCURITÉ PUBLIQUE DU CANADA, *Stratégie de cybersécurité du Canada. Renforcer le Canada et accroître sa prospérité*, 2010.

MINISTERE DE LA SECURITE PUBLIQUE DU CANADA, *Liste des entités terroristes inscrites*, disponible à l'adresse : http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-fra.aspx (consulté le 3 Avril 2014).

MINISTÈRE DE LA SÉCURITÉ PUBLIQUE CANADA, *Bâtir un Canada sécuritaire et résilient, le Centre Canadien de réponse aux incidents cybernétiques (CCRIC)*, Mai 2014, en ligne http://www.colloque-rsi.com/wp-content/uploads/2014/05/Frank-Turbide-RSI2014.pdf (consulté le 10 Octobre 2014).

MINISTERE DE LA SECURITE PUBLIQUE DU CANADA, *Liste des entités terroristes inscrites*, en ligne http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-fra.aspx (consulté le 3 Avril 2014).

PARLEMENT DU CANADA, *Livres blanc,* disponible à l'adresse : http://www.parl.gc.ca/parlinfo/Compilations/FederalGovernment/PaperList.aspx?Language=F&Menu=Fed-Doc-White&Paper=c6a4db8e-e464-430b-bbfe-ca77532e9ccb&Year=0&Department=&Minister=&Title=&Subject= (consulté le 15 Mars 2014).

PARLEMENT DU CANADA, « La cybersécurité et la cybercriminalité : s'attaquer à une menace complexe », Le monde numérique.

PARLEMENT DU CANADA, « Résumé législatif du projet de loi C-52 *: Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention* », 2011.

PARLEMENT DU CANADA, Division du droit et du gouvernement, « La « Patriot Act » des États-Unis et la *Loi Antiterroriste* du Canada : Principales différences entre les deux approches législatives », 2006.

PARLEMENT du CANADA, *Résumé législatif du projet de loi C-51 : Loi sur les pouvoirs d'enquête au 21e siècle*, Publication no 40-3-C51F, 3 Février 2011.

PARLEMENT du CANADA, *Résumé législatif du projet de loi C-47 : Loi sur l'assistance au contrôle d'application des lois au 21e siècle*, Publication n° LS-655F, 28 Juillet 2009.

PARLEMENT DU CANADA, *Résumé législatif du projet de loi C-13 : Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle***,** 11 Décembre 2013, (dernières révisions le 28 Août 2014).

PARLEMENT DU CANADA, Division du droit et du gouvernement, « La « Patriot Act » des États-Unis et la *Loi Antiterroriste* du Canada : Principales différences entre les deux approches législatives », **(**2006**)**, disponible à l'adresse : http://www.parl.gc.ca/content/lop/researchpublications/prb0583-f.htm (consulté le 15 Avril 2014).

SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ, Fiche documentaire no 13, *Le Centre intégré d'évaluation des menaces (CIEM)*, à l'adresse : http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr13-fra.pdf (consulté le 20 Août 2014).

SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ, *Rapport 2011-2013*, 2014.

SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ, *Réponse du SCRS aux questions additionnelles de la Commission*, question 3.

COMMISSARIAT DU CENTRE DE LA SECURITE DES TELECOMMUNICATIONS, *Rapport annuel 2012-2013*, Juin 2013.

Documents américains

U.S. DEPARTMENT OF STATE, *Foreign Terrorist Organizations*, September 28, 2012, disponible à l'adresse : http://www.state.gov/j/ct/rls/other/des/123085.htm (consulté le 3 Avril 2014).

DEPARTEMENT OF JUSTICE, USA PATRIOT Act: Preserving Life and Liberty, P.L. 107-56, 115 Stat. 272 **(**2001**),** disponible à l'adresse : http://www.justice.gov/archive/ll/highlights.htm (consulté le 15 Septembre 2014).

ORGANISATION DES ETATS AMÉRICAINS, *21 Steps to Improve Cyber Security of SCADA Networks*, U.S. Department of Energy, USA, **(**2002**)**, disponible à l'adresse : http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf.

ORGANIZATION OF AMERICAN STATES, disponible à l'adresse: http://www.oas.org/en/sms/cicte/programs_cyber.asp (consulté le 10 Mai 2014).

Documents européens

COMITÉ DES MINISTRES EUROPÉENS, *Décision n° CM/Del/Dec (97) 583.*

CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention sur la cybercriminalité*, STE no. 185, disponible à l'adresse : http://conventions.coe.int/treaty/fr/Reports/Html/185.htm (consulté le 16 Septembre 2014).

COUNCIL OF EUROPE, *Cyberterrorism-the use of the internet for terrorist purposes*, Strasbourg, Council of Europe publishing, 2007.

CONSEIL DE L'ORGANISATION POUR LE COMMERCE ET LE DEVELOPPEMENT ECONOMIQUE, *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information. Vers une culture de la sécurité*, 1037ème session, **(**juillet 2002**)**.

Documents internationaux

CONSEIL DE SÉCURITÉ, *Répertoire de la pratique du Conseil de sécurité*, **(**2010 – 2011), disponible à l'adresse : http://www.un.org/en/sc/repertoire/2010-2011/Particle%20III/2010-2011_Particle%20III.pdf#page=3 (consulté le 22 Septembre 2014).

Documents des organismes privés

ATCA, "Cyber Warfare– Beyond Estonia-Russia ATCA Briefings The Rise of China's 5th Dimension Cyber Army", 3 Mai 2007.

DELOITTE, *Cyber Espionage The harsh reality of advanced security threats*, Center for Security & Privacy Solutions, 2011.

Groupe CGI inc., Communiqué de presse, 2 avril 2013, Ottawa, disponible à l'adresse : http://www.cgi.com/fr/Cybersecurite-preoccupation-expertise-locale-mondiale-CGI-attenuer-niveau-risque (consulté le 5 Décembre 2014).

HUMAN RIGHT WATCH, *États-Unis : Les poursuites judiciaires liées au terrorisme sont souvent basées sur des motifs illusoires*, disponible à l'adresse : http://www.hrw.org/fr/news/2014/07/21/État s-unis-les-poursuites-judiciaires-liees-au-terrorisme-sont-souvent-basees-sur-de (consulté le 4 Septembre 2014).

IBM, *SCADA Security Solutions*, disponible à l'adresse : http://www-935.ibm.com/services/us/en/it-services/scada-security-solutions.html (consulté le 14 Avril 2014).

INFORMATION WARFARE MONITOR, *Tracking GhostNet: Investigating a cyber espionage network*, Canada, 2009.

INFORMATION WARFARE MONITOR AND SHADOWSERVER*, Shadows in the cloud: Investigating cyber espionage 2.0*, 2010, disponible à l'adresse : http://www.nartv.org/mirror/shadows-in-the-cloud.pdf (consulté le 14 Avril 2014).

PALO ALTO, Networks DNS protection mecanisms, disponible à l'adresse: http://fr.slideshare.net/MarcelloMarchesini/dns-protection (consulté le 10 Janvier 2014)

SECURITY & DEFENCE AGENDA*, Cyber-security: The vexed question of global rules An independent report on cyber-preparedness around the world*, Geert Cami, Février 2012.

SYMANTEC, *The Nature of Cyber Espionage: Most Malicious File Types Identified and Encrypted Spam from Rustock*, **(**2010**),** MessageLabs Intelligence, disponible à l'adresse: http://www.messagelabs.com/mlireport/MLI_2010_03_Mar_FINAL-EN.pdf (consulté le 1 Avril 2014).

MANDIANT, *APT1 Exposing One of China's Cyber Espionage Units,* 2004.

UNIVERSITÉ DE SORBONNE, « Exposé des motifs du projet de loi relatif à la transposition de la *Convention* de Budapest en droit français », disponible à l'adresse : http://www.univ-paris1.fr/diplomes/master-droit-du-numerique/bibliotheque-numerique-du-droit-de-ladministration-electronique/tic/informatique/cybercriminalite/expose-des-motifs-du-projet-de-loi-relatif-a-la-transposition-de-la-*Convention*-de-budapest-en-droit-francais/ (consulté le 20 Septembre 2014).

Articles de journaux

ALTESE, L., « Cybercriminalité : un fléau en hausse en France ! », **(**14 Décembre 2014**)**, disponible en ligne : http://blog.economie-numerique.net/2012/12/14/cybercriminalite-un-fleau-en-hausse-en-france/ (consulté le 5 Avril 2014)

BALL, J., « US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data », 20 Novembre 2013.

BERNARD, P. et C. LESNES, « Une cyberattaque américaine aurait visé l'Élysée », 22 Novembre 2012, Le Monde.fr, disponible à l'adresse : http://www.lemonde.fr/international/article/2012/11/22/une-cyberattaque-americaine-aurait-vise-l-elysee_1794150_3210.html (consulté le 20 Octobre 2013).

BROAD, W. J. et D. E. SANGER, « Worm aws perfect for sabotaging centrifuges », 18 Novembre 2010, New York Times.

CAMERON, D., « Vague de cyberespionnage: quatre cibles au Canada visées », 04 août 2011, LaPresse.ca, disponible à l'adresse : http://www.lapresse.ca/actualites/justice-et-affaires-criminelles/201108/04/01-4423318-vague-de-cyberespionnage-quatre-cibles-au-canada-visees.php (consulté le 15 Avril 2014).

CROUZILLACQ, P., « GhostNet, le cyber-espion qui venait de Chine», disponible à l'adresse : www.01net.com/editorial/500430/ghostnet-le-cyber-espion-qui-venait-de-chine/ (consulté le 14 Mars 2014).

DEIBERT, R., *Militarizing Cyberspace To preserve the open Internet we must stop the cyber arms race*, 22 Juin 2010, disponible à l'adresse: http://www.technologyreview.com/notebook/419458/militarizing-cyberspace/ (consulté le 17 Octobre 2014)

DOORNBOS, H. et J. MOUSSA, « Ce que l'on trouve dans l'ordinateur portable d'un membre de l'État islamique », 2014, disponible à l'adresse : http://www.slate.fr/story/91569/ordinateur-portable-membre-etat-islamique (consulté le 15 Septembre 2014).

DORIGNY, M., « Le projet NSA-Observer », 28 Juillet 2014, disponible à l'adresse: http://www.information-security.fr/projet-nsa-observer/ (consulté le 20 Septembre 2014).

FARREL, P., « History of 5-Eyes – explainer », 2 Décembre 2013, disponible à l'adresse : http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer (consulté le !) Janvier 2014)

FOLLOROU, J. et M. UNTERSINGER, « La France suspectée de cyberespionnage », 26 Mars 2014, Le Monde.fr, disponible à l'adresse : www.lemonde.fr/international/article/2014/03/21/la-france-suspectee-de-cyberattaque_4387232_3210.html (consulté le 1 Avril 2014).

FoxNews.com, « Anonymous hacking group targeting government websites, FBI warns », 17 Novembre 2013, disponible à l'adresse : http://www.foxnews.com/tech/2013/11/17/anonymous-hacking-group-targeting-government-websites-fbi-warns/ (consulté le 3 Avril 2014).

France Tv, Reportage sur l'affaire MERAH, Itinéraire d'un tueur, , disponible à l'adresse : https://www.youtube.com/watch?v=Q3GS0d0N390 (consulté le 17 Octobre 2014).

GAGNON B., Interview par Jean-François LISÉE, disponible à l'adresse : https://www.youtube.com/watch?v=4rA9AzSEHXM (consulté le 7 Janvier 2015).

GREENEMEIER, L., « Electronic Jihad' App Offers Cyberterrorism For The Masses », 7 Juillet 2007, disponible à l'adresse : http://www.informationweek.com/electronic-jihad-app-offers-cyberterrorism-for-the-masses/d/d-id/1056683 (consulté le 17 Août 2014).

HAQUET, C. et E. PAQUETTE, « NSA: les Américains étaient-ils à l'origine de l'espionnage de l'Elysée en 2012? », 20 Novembre 2012, disponible à l'adresse : http://lexpansion.lexpress.fr/high-tech/nsa-les-americains-etaient-ils-a-l-origine-de-l-espionnage-de-l-elysee-en-2012_1340421.html (consulté le 5 mai 2013).

ITespresso.fr, « Et si une cyberattaque causait la perte d'une nation ? », 30 Octobre 2014, en ligne http://www.itespresso.fr/cyberattaque-causait-perte-nation-80719.html (consulté le 13 Décembre 2014).

KALLERBORN, G., « Cybercriminalité: les forces de l'ordre en formation continue », **(**21 Janvier 2014**)**, disponible à l'adresse : http://www.01net.com/editorial/612428/cybercriminalite-les-forces-de-lordre-en-formation-continue/ (consulté le 18 Août 2014)

Ledevoir.com, « Le FBI a poussé des Américains musulmans à commettre des attentats », disponible à l'adresse : http://www.ledevoir.com/international/État s-unis/414010/État s-unis-le-fbi-a-pousse-des-americains-musulmans-a-commettre-des-attentats (consulté le - Décembre 2014)

LeMonde.fr avec AFP, « Des pirates informatiques russes auraient volé plus d'un milliard de mots de passe », **(**6 Août 2014**)**, en ligne

http://www.lemonde.fr/pixels/article/2014/08/06/des-pirates-informatiques-russes-auraient-vole-plus-d-un-milliardv-de-mots-de-passe_4467212_4408996.html (consulté le 6 Août 2014).

LeMonde.fr ; « Etats-Unis : un ex-général soupçonné de fuites sur une cyberattaque contre l'Iran », 28 Juin 2006.

MALBRUNOT, G., « De Fukushima à Stuxnet en Iran, les effets collatéraux de la cyberguerre », 4 Avril 2012, disponible à l'adresse : http://blog.lefigaro.fr/malbrunot/2011/04/de-fukhushima-a-stuxnet-en-ira-1.html (consulté le 13 Décembre 2014).

MARKOFF, J. and D. BARBOZA, « 2 China Schools Said to Be Tied to Online Attacks », **(**February 18, 2010**)**, NYTimes.com, disponible à l'adresse : http://www.nytimes.com/2010/02/19/technology/19china.html?_r=0 (consulté le 5 Février 2014).

MIKKO, H., « Fending off attacks in cyberspace, the global nature of cyberwarfare », May 29, 2009, NYTimes.com, disponible à l'adresse: http://roomfordebate.blogs.nytimes.com/2009/05/29/a-plan-of-attack-in-cyberspace/ (consulté le 4 Mars 2014).

OBAMA, B., « Taking the Cyberattack Threat Seriously », July 19, 2012, The Wall Street Journal, disponible à l'adresse: http://www.wsj.com/video/taking-the-cyberattack-threat-seriously/ED29A414-7BAA-423F-8F9B-9AD49930F8F3.html?KEYWORDS=cyberattack+Obama (consulté le 2 Août 2014).

PANETTA, A., « Les autorités américaines créent des terroristes, selon une étude », 21 Juillet 2014, en ligne : http://www.lactualite.com/actualites/monde/les-autorites-americaines-creent-des-terroristes-selon-une-etude/ (consulté le 16 Août 2014).

Pièce à conviction, *Anonymous, la guerre est déclarée*, disponible à l'adresse : https://www.youtube.com/watch?v=mpHJwW258gs (consulté le 12 Octobre 2014).

PILLOU, J.F., « Les bombes logiques », 2014, disponible à l'adresse : « http://www.commentcamarche.net/contents/1223-bombes-logiques#q=bombes+logiques&cur=1&url=%2F » (consulté le 7 Juin 2014).

Radio-Canada avec Reuters et La Presse canadienne, « Cyberattaque chinoise contre le Conseil national de recherches », 29 juillet 2014, disponible à l'adresse : http://ici.radio-canada.ca/nouvelles/National/2014/07/29/001-cnrc-cyberattaque-chinoise.shtml (consulté le 30 Juillet 2014).

Radiocanada.ca, « Cyberattaque au CNRC : un système de données personnelles touché », 31 Juillet 2014, disponible à l'adresse : http://ici.radio-canada.ca/nouvelles/societe/2014/07/31/003-comissaire-vie-privee-cyberattaque-cnrc-pirates-acces-systeme-renseignements-personnelles.shtml (consulté le 10 Août 2014).

Radiocanada.ca, « De jeunes Québécois soupçonnés d'avoir rejoint des djihadistes en Syrie », disponible à l'adresse : http://ici.radio-canada.ca/nouvelles/societe/2015/02/25/006-jeunes-quebecois-quitte-pays-syrie-djihadistes.shtml (consulté le 12 Février 2015).

Rtbf.be, « Le méga-procès pour terrorisme de Sharia4Belgium se poursuit à Anvers », disponible à l'adresse : http://www.rtbf.be/info/belgique/detail_le-proces-pour-terrorisme-de-sharia-for-belgium-debute-a-anvers?id=8366206 (consulté le 12 Octobre 2014)

SANGER, D. E., « Iran fights malware attacking computers », 25 Septembre 2010, New York Times.

SHANE, S., « La NSA mise à nu », 14 Novembre 2013, The NYTimes.com, disponible à l'adresse : http://www.courrierinternational.com/article/2013/11/14/la-nsa-mise-a-nu (consulté le 4 Avril 2014).

TAKAHASHI, D., « Defcon air traffic control hacker: Excuse me while I change your aircraft's flight plan», August 1, 2009, Venturebeat, disponible à l'adresse: http://venturebeat.com/2009/08/01/defcon-hacker-excuse-me-while-i-change-your-aircrafts-flight-plan/ (consulté le 3 Avril 2014)

THORNBURGH, N., « The Invasion of the Chinese Cyberspies », TIME, 29 Août 2005

Dictionnaires

CORNU Gérard (dir.), Vocabulaire juridique, 8ème, Paris, Association Henri Capitant, P.U.F., 2007.

OFFICE DE LA LANGUE FRANCAISE, « Le grand dictionnaire terminologique », (2002), disponible en ligne http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8354359 (consulté le 3 Septembre 2014)