BIBLIOTHÈQUE du PARLEMENT
LIBRARY of PARLIAMENT

ÉTUDE GÉNÉRALE

Cybersécurité et renseignement de sécurité : L'approche des États-Unis

Publication n^{o} 2010-02-F
Révisée le 15 juin 2011

Holly Porteous

Division des affaires internationales, du commerce et des finances
Service d'information et de recherche parlementaires

Cybersécurité et renseignement de sécurité : L'approche des États-Unis

(Étude générale)

La présente publication est aussi affichée en versions HTML et PDF sur IntraParl (l'intranet parlementaire) et sur le site Web du Parlement du Canada.

Dans la version électronique, les notes de fin de document contiennent des hyperliens intégrés vers certaines des sources mentionnées.

This publication is also available in English.

Les ***études générales*** de la Bibliothèque du Parlement présentent et analysent de façon objective et impartiale diverses questions d'actualité sous différents rapports. Elles sont préparées par le Service d'information et de recherche parlementaires de la Bibliothèque, qui effectue des recherches et fournit des informations et des analyses aux parlementaires ainsi qu'aux comités du Sénat et de la Chambre des communes et aux associations parlementaires.

Publication n^{o} 2010-02-F
Ottawa, Canada, Bibliothèque du Parlement (2011)

TABLE DES MATIÈRES

CYBERSÉCURITÉ ET RENSEIGNEMENT DE SÉCURITÉ : L'APPROCHE DES ÉTATS-UNIS

1 INTRODUCTION

Des allégations faites en janvier 2010 selon lesquelles la Chine aurait piraté les comptes de courriel de Google et les systèmes informatiques d'au moins 33 autres entreprises américaines mettent en lumière une campagne continue de cyberespionnage de plus en plus audacieuse menée contre les intérêts des États-Unis et de leurs alliés [1]. En effet, les soupçons de cyberespionnage qui pèsent contre la Chine ont d'abord attiré l'attention du public en 2003, lorsque des rapports sont venus affirmer que celle-ci était à l'origine d'une opération massive et coordonnée qui avait compromis la sécurité de systèmes informatiques confidentiels des gouvernements et du secteur privé aux États-Unis, au Royaume-Uni, en Australie, en Nouvelle-Zélande et au Canada. Qualifiée de « Pluie de Titan » aux États-Unis, cette opération d'espionnage n'a jamais vraiment cessé [2]. Elle s'est seulement transformée en attaques constantes, au moyen d'une vaste infrastructure secrète de systèmes compromis, contre les États-Unis, leurs partenaires des Five Eyes [3] (le Canada, le Royaume-Uni, l'Australie et la Nouvelle-Zélande) et d'autres pays. La Chine est l'un des États de plus en plus nombreux dont on croit qu'ils se servent d'Internet pour voler des renseignements classifiés ou exclusifs et, selon de nombreux analystes, à préparer des actes de sabotage en prévision d'un conflit [4].

Les États-Unis, considérant le cyberespionnage et les cyberattaques comme des menaces de premier ordre, ont reformulé leur stratégie nationale en matière de cybersécurité. Trois de leurs plus proches partenaires du milieu du renseignement (Five Eyes) – l'Australie, la Nouvelle-Zélande et le Royaume-Uni – leur ont emboîté le pas. En 2004, le Canada a lui aussi commencé à préparer une stratégie nationale en matière de cybersécurité, mais, au moment où nous écrivons ces lignes, il n'a pas encore fait connaître publiquement sa position. Puisque l'expérience qu'ont connue les États-Unis a profondément influé sur les stratégies de leurs alliés, le présent document se concentrera sur leur approche. Pour des raisons qui seront explorées plus loin dans ce document, le renseignement sur les transmissions (SIGINT – interception de signaux électroniques de tout genre en vue de réunir des renseignements sur une cible) y joue un rôle central.

2 ENCADREMENT DE LA QUESTION

On sait depuis un certain temps déjà que les cyberattaques peuvent faire des ravages sur une grande échelle [5]. On attribue souvent la première attaque automatisée à Robert T. Morris. En 1988, celui-ci avait envoyé le ver informatique Morris dans le réseau ARPANET (le prédécesseur d'Internet) [6]. Le ver, après avoir infecté environ 60 000 ordinateurs utilisant un système d'exploitation de type Unix, a entraîné la mise en place d'une équipe d'intervention d'urgence en informatique à l'Université Carnegie Mellon et a valu à son créateur trois années de probation, 400 heures de service communautaire et une amende de 10 000 $US. Néanmoins, il aura fallu une décennie avant que, sous le gouvernement Clinton, l'on fasse une

tentative concertée de réfléchir à la cybersécurité à l'échelle nationale; elle a été le fait de la Commission on Critical Infrastructure Protection, présidée par Robert Marsh, général retraité des Forces armées américaines. Les recommandations présentées par la Commission Marsh en 1997 sur la dimension informatique de la protection des infrastructures essentielles, constituaient le fondement de la Presidential Decision Directive 63 (directive présidentielle ou PDD 63), laquelle, à son tour, donnait un cadre à la question de la cybersécurité et aux intentions du gouvernement. Chose remarquable, malgré une série de mises à jour effectuées par les gouvernements successifs (le National Plan for Information Systems Protection, en 2000, la National Strategy to Secure Cyberspace en 2003, la Comprehensive National Cybersecurity Initiative en 2007, et la Cyberspace Policy Review en 2009), les thèmes fondamentaux établis dans la PDD 63 demeurent. Ils sont les suivants :

1. L'ampleur du dossier exige la participation de l'exécutif et la mise en place de structures de gouvernance pour appuyer une coordination complexe des politiques et des opérations.
2. La Défense nationale, les Affaires étrangères ainsi que les organismes du renseignement et d'application de la loi sont les organismes responsables.
3. L'interconnectivité des systèmes public et privé exige l'adoption d'une approche globale qui touche l'ensemble de la société et la mise sur pied de partenariats entre les secteurs public et privé.
4. Il faut faire comprendre la cybersécurité aux secteurs public et privé par l'éducation et la sensibilisation.
5. Les exploitants du secteur privé sont les mieux placés pour décider de la façon d'assurer la sécurité de leurs systèmes. Lorsqu'on collabore avec eux, on devrait privilégier les mesures incitatives plutôt que la réglementation. Cependant, on aura recours à des lois et à des règlements au besoin.
6. Il faut respecter la protection de la vie privée et préserver la confidentialité des renseignements mis en commun.
7. Compte tenu de l'envergure planétaire et de la nature supranationale d'Internet, le succès de la mise en œuvre de la politique passe par la coopération internationale.
8. Il faut mener des activités de recherche et de développement pluriannuelles parrainées par le gouvernement fédéral afin de remédier aux vulnérabilités informatiques.
9. Le gouvernement fédéral doit d'abord assurer sa propre sécurité pour faire œuvre de pionnier dans l'établissement de pratiques exemplaires[7].

3 APPLICATION DE LA STRATÉGIE : CHOISIR L'OUTIL APPROPRIÉ

3.1 L'APPLICATION DE LA LOI PREND LA TÊTE

Si l'énoncé du problème a peu changé depuis la publication de la PDD 63 en 1998, tel n'est pas le cas des instruments utilisés pour le régler. Avant la Comprehensive

National Cybersecurity Initiative de 2007, l'application de la loi était l'« outil par excellence ». Par exemple, la PDD 63 comptait sur le tout nouveau National Infrastructure Protection Center (NIPC) pour la préalerte et l'intervention. Le NIPC, établi en février 1998 par le département de la Justice et le Federal Bureau of Investigation (FBI), avait pour mission de collaborer avec le secteur privé, les États et les autorités locales ainsi que d'autres organismes responsables du fédéral – y compris des organismes de défense et de renseignement – afin d'évaluer les menaces, de donner l'alerte, de déterminer la vulnérabilité, de mener des enquêtes pour l'application de la loi et de réagir aux cyberincidents touchant les infrastructures essentielles. Le NIPC était composé principalement d'agents du FBI, mais d'autres départements et organismes de renseignement du fédéral ainsi que le Canada, l'Australie et le Royaume-Uni lui ont aussi fourni du personnel [8].

Il est révélateur que la Stratégie nationale de 2003 ait cherché à améliorer la capacité des forces de l'ordre de prévenir la cybercriminalité et de traduire en justice ceux qui s'en rendent coupables. Il était en effet devenu évident que le modèle du NIPC ne tenait pas ses promesses. Par exemple, en 2000, tout en louant les initiatives déployées par le Centre sur le plan des enquêtes, de la formation et de la sensibilisation, le General Accounting Office (GAO – maintenant le Government Accountability Office) a déclaré au Congrès que le NIPC présentait de graves lacunes au chapitre de ses capacités d'analyse et d'alerte [9]. De fait, le NIPC n'a réussi à diffuser un avertissement au sujet du virus de sinistre mémoire « ILOVEYOU » que plusieurs heures après que des départements du gouvernement et des organismes privés ont commencé à succomber à l'attaque [10]. À ce sujet, le GAO a aussi noté que le secteur privé hésitait à communiquer au NIPC des renseignements sur les incidents parce qu'il craignait que le FBI soit plus désireux de traduire en justice ceux qui s'en étaient rendu coupables que de protéger le caractère confidentiel de l'information. L'approche adoptée par le NIPC, soit celle d'un « centre de convergence », visait à fournir une réaction coordonnée, mais il était manifeste que le seul fait de réunir sous un même toit des représentants d'organismes différents ne suffisait pas à surmonter les problèmes de mandats divergents, d'échange d'information et de manque de clarté des rôles et des responsabilités. À l'aide de la Stratégie nationale, on a tenté de dénouer le problème en intégrant le NIPC dans le nouveau département de la Sécurité intérieure. Cependant, les problèmes sous-jacents demeuraient. Alors que des États, des organisations criminelles, des sociétés et des particuliers peuvent tous s'adonner à la cybercriminalité et à la cyberguerre, les organismes d'application de la loi sont équipées pour répondre à quelques-unes de ces menaces, mais non à toutes.

3.2 LE RENSEIGNEMENT DE SÉCURITÉ SE JOINT À LA MÊLÉE

La Comprehensive National Cybersecurity Initiative (CNCI) de 2007, rendue publique après un examen de la Stratégie nationale de 2003, annonçait la fin du rôle prépondérant joué par l'élément d'application de la loi [11]. Celui-ci devait demeurer un élément essentiel de la cybersécurité, mais il s'agirait dorénavant d'un élément parmi tant d'autres. Selon Melissa Hathaway, ex-chef de la cybersécurité au Conseil national de sécurité des États-Unis : « Il est fondamental, dans cette stratégie, de "rapprocher" les missions de cyberdéfense, traditionnellement distinctes, des capacités en matière d'application de la loi, de renseignement, de contre-espionnage et d'activité

militaire afin de tenir compte de toutes les cybermenaces, allant des intrusions à distance dans les réseaux et des exploitations non autorisées de l'intérieur, jusqu'aux vulnérabilités de la chaîne d'approvisionnement [12]. »

Bref, la CNCI vise une utilisation plus efficace du « coffre à outils » de la cyberdéfense. Chacun des « outils » – organismes d'application de la loi, forces armées et organismes de renseignement – doit jouer un rôle dans la protection des systèmes informatiques américains contre les cybermenaces. Le FBI fournit au secteur privé des conseils dont celui-ci a grandement besoin pour assurer sa sécurité. Il mène des enquêtes sur la cybercriminalité et intente des poursuites contre ceux qui s'en rendent coupables, y compris dans les cas de cyberespionnage, ce qui génère d'importants renseignements de contre-espionnage et aide à décourager d'autres criminels éventuels. Les organismes des forces armées et du renseignement apportent une dimension différente et plus opérationnelle à la cyberdéfense. Par exemple, avec son nouveau cybercommandement (CYBERCOM), le département américain de la Défense se prépare à participer à un ensemble complet d'opérations de réseaux informatiques – de la défense à l'exploitation non autorisée et à l'attaque [13]. Le hasard n'a rien à voir avec la nomination du général Keith Alexander, directeur de la National Security Agency (NSA) des États-Unis, à la direction de CYBERCOM. Comme nous le verrons plus en détail, la NSA (une agence du département de la Défense) jouit de pouvoirs considérables.

Les organismes d'application de la loi, les forces armées et les organismes de renseignement ont chacun une mission en matière de cyberdéfense, mais leurs pouvoirs respectifs exercent différentes contraintes sur la portée de leurs activités. Par exemple, les médias ont rapporté que l'enquête menée par le FBI sur l'attaque de la Pluie de Titan a été entravée par le refus de la Chine de collaborer et par la réticence du gouvernement américain à autoriser le FBI à recourir à l'exploitation non autorisée de réseaux informatiques (CNE) [14] pour enquêter. D'autres entités, comme les forces armées, ont des règles d'engagement moins strictes en ce qui concerne la CNE contre des entités étrangères. Ce qui les préoccupe principalement, c'est de ne pas se faire prendre [15].

Dans le contexte national, toutefois, l'armée américaine se heurte à ses propres contraintes. C'est pourquoi les fonctionnaires du département de la Défense ont divisé la tâche de la cyberdéfense entre militaires et civils, expliquant que CYBERCOM serait responsable de la sécurité des sites Web du domaine « .mil » (le domaine de tête à l'usage exclusif des militaires américains), tandis que le département de la Sécurité intérieure superviserait les mesures de sécurité des sites Web du domaine « .gov » (le domaine de tête à l'usage exclusif du gouvernement des États-Unis) [16]. Néanmoins, Einstein – un système de surveillance du trafic sur les réseaux qui est en voie d'élaboration et qui permettra d'assurer la sécurité du domaine « .gov » – est un exemple de certains des problèmes juridiques et politiques complexes soulevés par le « rapprochement » des missions. Einstein est exploité par le département de la Sécurité intérieure, mais dépend des signatures d'attaque fournies par la NSA [17]. À l'heure actuelle, le système commence à dépasser le simple fait de surveiller et de signaler les échanges potentiellement néfastes sur le réseau Internet en partance ou à destination des ministères gouvernementaux pour passer à l'interception active de ces échanges [18]. Les

signatures d'attaque fournies par la NSA déclenchent une opération de « perquisition et saisie » automatisée des échanges suspects, mais sous l'autorité ultime du département de la Sécurité intérieure.

3.3 PLUS D'ATTENTION À LA GOUVERNANCE, AUX MESURES LÉGISLATIVES ET AUX POLITIQUES

Une des premières mesures que Barack Obama a prises à titre de président a été de commander un examen de 60 jours de la politique américaine sur la cybersécurité. Le Cyberspace Policy Review [19] qui en a résulté en mai 2009 confirmait le rapprochement par la CNCI des missions de défense, de renseignement et d'application de la loi, auparavant distinctes. Elle énonçait aussi dix mesures à court terme [20], liées pour la plupart à la gouvernance, aux lois et aux politiques. Si l'on considère que les États-Unis se préparent à adopter une approche plus opérationnelle à l'égard de l'exploitation non autorisée agressive de réseaux informatiques, on ne devrait pas s'en surprendre. Pour prendre des décisions de façon quasi instantanée au beau milieu d'attaques rapides provenant de plusieurs pays, il faut définir clairement les rôles et les responsabilités et se doter d'une solide assise juridique et politique.

Si les grands thèmes de la stratégie en matière de cybersécurité n'ont pas beaucoup changé depuis la PDD 63, tel n'est pas le cas du sentiment d'urgence. Les cybermenaces qui, en 1998, semblaient un peu théoriques à plusieurs sont devenues une réalité tangible. Aucun « Pearl Harbour informatique » ne s'est encore produit, mais, depuis dix ans, les composantes informatiques clés sont de plus en plus fabriquées à l'étranger, ce qui laisse entrevoir l'inquiétante possibilité que les logiciels des systèmes essentiels soient dotés d'une capacité d'autodestruction. Le cyberespionnage a entraîné des pertes économiques réelles, et la rapidité, le volume et la nature coordonnée de ces intrusions ont fait voir la nécessité de connaître la situation en temps réel afin d'y réagir de façon efficace. C'est pourquoi on note, dans la volonté manifestée par la CNCI de protéger le gouvernement contre les attaques, le désir d'adopter une approche opérationnelle semblable à celle qui est nécessaire pour mener combat. L'établissement de CYBERCOM en 2009 porte à croire que c'est précisément le cas.

4 POURQUOI LE RENSEIGNEMENT DE SÉCURITÉ GAGNE EN IMPORTANCE

Comme nous l'avons souligné, la façon de voir les mécanismes de mise en œuvre de la stratégie ont changé. Au début, l'application de la loi primait. Par exemple, la PDD 63, tout en reconnaissant que certains cyberincidents auraient une portée nationale nécessitant la participation des agences de renseignement, confiait au FBI, un organisme d'application de la loi, la direction du système national d'avertissement et de partage de l'information. En outre, les États-Unis (ainsi que le Canada) étaient activement à la recherche de solutions diplomatiques, mais surtout pour formuler des normes internationales de sécurité technique et criminaliser certaines cyberactivités par l'entremise de la Convention sur la cybercriminalité du Conseil de l'Europe [21].

L'application de la loi demeure un instrument important de la cybersécurité nationale, mais principalement pour ce qui est de sensibiliser la population et d'intenter des actions en justice en cas de cybercrimes ayant leur origine au pays ou dans un pays disposé à appuyer l'enquête. Malgré l'entrée en vigueur de la Convention sur la cybercriminalité en 2004, les poursuites judiciaires à l'échelle internationale imposent un travail de longue haleine. Les démantèlements de réseaux internationaux de pornographie juvénile, très médiatisés, sont contrebalancés par des résultats décevants, comme l'incapacité de traîner devant la justice toutes les personnes responsables de l'inondation massive des systèmes gouvernementaux et financiers de l'Estonie en 2007. Si l'on en juge d'après l'échange enflammé intervenu entre la Chine et les États-Unis, il est peu vraisemblable que la solution juridique aux attaques survenues contre Google et d'autres entreprises américaines soit entièrement satisfaisante [22]. La menace de poursuites – faible à cause de l'impossibilité de découvrir avec certitude les sources de l'attaque, des différences entre les législations des divers pays et le manque de coopération – ne suffit pas à dissuader les États de s'adonner au cyberespionnage. Les risques sont trop faibles, et les avantages sur le plan du renseignement, trop élevés. Tant qu'on ne pourra découvrir les auteurs des attaques de façon fiable grâce à des systèmes de gestion de l'identité, un problème qui, d'après le Cyberspace Policy Review, exige d'être réglé à court terme, les cyberpirates profiteront de la protection offerte par des pays qui n'ont pas signé la Convention sur la cybercriminalité, comme la Chine et la Russie, et pourront agir relativement en toute impunité. Les experts s'entendent pour dire que, devant cette réalité, il faudra renforcer le mécanisme essentiellement réactif qu'est l'application de la loi en renforçant également les mesures préventives, y compris la préalerte, et en élaborant un plus large éventail de moyens d'action. C'est pour cette raison que le renseignement de sécurité, notamment celui fourni par la NSA, a gagné en importance.

Le public a tendance à associer la NSA à la seule collecte de renseignements touchant l'étranger – une association qui n'aide pas à dissiper les craintes que ses responsabilités de haut niveau découlant de la nouvelle stratégie de cybersécurité menacent le droit à la vie privée [23]. Cependant, l'Agence a depuis longtemps pour mandat d'aider à défendre les renseignements et les réseaux informatiques les plus délicats des États-Unis. Les agences de SIGINT comme la NSA sont bien placées pour lancer des avertissements, notamment contre les cyberintrusions complexes perpétrées par des États, parce qu'elles s'adonnent elles-mêmes constamment à ces mêmes activités. La CNE est devenue un outil indispensable de collecte de renseignements touchant l'étranger pour de nombreuses agences de SIGINT, dont celles des Five Eyes [24]. Pour gagner à ce jeu, les agences de SIGINT consacrent beaucoup de temps et d'énergie à explorer et à exploiter les points faibles des systèmes informatiques souvent bien endurcis de leurs cibles. Les connaissances qu'elles en tirent leur sont aussi très utiles lorsqu'il s'agit de déterminer si une entité tout aussi complexe tente de leur rendre la pareille. Le fait de détecter, puis d'observer tranquillement le travail de cyberintrus parrainés par un État qui essaient de voler ou d'altérer des données permet de recueillir des renseignements utiles sur leurs capacités et leurs intentions qui peuvent ensuite devenir des indicateurs et des avertissements au sujet des futures cibles.

Nous ne voulons pas laisser entendre que l'excellent point de vue qu'a la NSA des cybermenaces soit toujours confortable. Il existe des tensions évidentes entre ses activités de défense et d'exploitation non autorisée. Il en va de même de l'utilisation des compétences d'exploitation à des fins d'attaque. Un partage trop large de ce qu'elle sait au sujet des vulnérabilités informatiques exploitables pourrait bien un jour lui fermer l'accès à de précieux renseignements touchant l'étranger. Vu le nombre d'intérêts divergents en jeu parmi les organismes responsables, l'on comprendra qu'un problème de gouvernance ait subsisté d'une administration à l'autre.

5 CONCLUSION

Les États-Unis ont été parmi les premiers à assimiler la cybersécurité à une question de sécurité nationale et à élaborer des stratégies visant à lutter contre la série de menaces connexes. À mesure qu'ils se tournent de plus en plus vers des organismes des forces armées et du renseignement de sécurité pour fournir des préalertes et trouver d'autres moyens d'action, il va de soi que leurs plus proches alliés font de même. Par exemple, trois des agences de SIGINT des partenaires Five Eyes de la NSA – le Government Communications Headquarters au Royaume-Uni, la Defence Signals Directorate en Australie et le Government Communications Security Bureau en Nouvelle-Zélande – ont des responsabilités du même ordre dans le cadre des stratégies de cybersécurité de leur gouvernement respectif [25]. Comme nous l'avons déjà mentionné, le Canada n'a pas encore formulé sa stratégie, mais des rapports laissent présager son annonce imminente [26].

Les capacités des agences de SIGINT comme la NSA ne font aucun doute, mais des questions importantes subsistent quant à la façon dont on peut utiliser ces capacités pour aider à assurer la cybersécurité au-delà du fédéral. Comme la Chine l'a noté indirectement dans sa riposte aux déclarations publiques de la secrétaire d'État Clinton au sujet de l'attaque contre Google, il existe aussi une contradiction indéniable (mais non insurmontable) entre amener la communauté internationale à collaborer pour lutter contre la cybercriminalité et exercer ce genre d'activité au niveau de l'État [27]. Enfin, les États-Unis s'efforcent d'intégrer l'exploitation non autorisée des réseaux informatiques, y compris l'attaque de ces réseaux, à leur planification militaire, ce qui a pour leur secteur privé et leurs alliés des conséquences qui doivent être explorées [28].

Les intérêts du Canada à l'égard de la stratégie américaine de cybersécurité sont multiples et touchent les deux pays. Au-delà des partenariats étroits qui existent entre ceux-ci sur le plan des forces armées, du renseignement et de l'application de la loi, le Canada et les États-Unis ont en commun de nombreuses infrastructures essentielles. Il vaudrait aussi la peine d'explorer les questions de souveraineté soulevées par l'intention qu'a le gouvernement des États-Unis de réglementer un plus grand nombre d'aspects des pratiques et des autres activités liées à la cybersécurité dans le secteur privé. Cependant, ces questions dépassent de beaucoup la portée du présent document [29].

NOTES

1. Pour connaître le détail de l'attaque et savoir qui était ciblé, voir Ariana Eunjung Cha et Ellen Nakashima, « Google China cyberattack part of vast espionage campaign, experts say », *Washington Post*, 14 janvier 2010; Dan Goodwin, « IE zero-day used in Chinese cyber assault on 34 firms », *The Register*, 14 janvier 2010.

2. La revue *TIME* a été parmi les premières à décrire en détail la Pluie de Titan. Voir Nathan Thornburgh, « The Invasion of the Chinese Cyberspies », *TIME*, 29 août 2005. Pour des reportages plus récents sur les soupçons d'espionnage informatique pesant contre la Chine, voir Brian Grow, Keith Epstein et Chi-chu Tschang, « The New E spionage Threat », *BusinessWeek*, 10 avril 2008; John Markoff, « Vast Spy System Loots Computers in 103 Countries », *New York Times*, 28 mars 2009. L'article de Markoff portait sur des recherches menées par le « Citizen Lab » de l'Université de Toronto, et le SecDev d'Ottawa, qui se trouvent dans Ron Deibert et Rafal Rohozinski, « Tracking GhostNet: Investigating a Cyber Espionage Network », 29 mars 2009. Pour lire l'histoire complète des cyberopérations chinoises, voir Bryan Krekel, « Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation », US-China Economic and Security Review Commission, 9 octobre 2009.

3. L'expression « Five Eyes » désigne les paires d'« yeux » autorisées à voir les renseignements. Par exemple, si un document est classifié « Pour citoyens canadiens seulement », cela signifie qu'il est interdit d'en faire part à des non-Canadiens. L'alliance des Five Eyes en matière de renseignements découle de l'entente de 1948 entre le Royaume-Uni et les États-Unis sur le renseignement (« traité UKUSA »). Voir Matthew Aid, *The Secret Sentry: The Untold History of the National Security Agency*, New York, Bloomsbury Press, 2009, et Christopher Andrew, « The Making of the Anglo-American SIGINT Alliance », dans Hayden Peake et Samuel Halpern (dir.), *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer*, Washington (D.C.), NIBC Press, 1994, p. 95 à 109.

4. Dans sa plus récente évaluation annuelle des menaces présentée à la commission sénatoriale des forces armées, la Defense Intelligence Agency des États-Unis a jugé que la Russie représentait la cybermenace la plus importante pour les États-Unis. Voir lieutenant-général Michael D. Maples, directeur de l'armée américaine, Defense Intelligence Agency, « Annual Threat Assessment », déclaration faite devant la commission sénatoriale américaine des forces armées, 10 mars 2009, p. 37.

5. Cependant, la possibilité qu'une cyberattaque en soi ruine un pays est controversée. Des observateurs de longue date comme Martin Libicki soulignent que, comme elles se fondent sur les vulnérabilités causées par des erreurs de codification, les armes informatiques sont parfaitement susceptibles de faire l'objet de parades. Une fois qu'une vulnérabilité aura été exposée, que ce soit grâce à une vigilance normale en matière de sécurité des télécommunications ou parce qu'elle aura été utilisée dans une cyber-attaque, on fera tout pour l'éliminer. Martin Libicki, *Cyberdeterrence and Cyberwar*, RAND Project Air Force, RAND Corporation, 2009.

6. Le premier programme informatique malveillant était le virus « Elk Cloner », qui a été programmé en 1982 par Richard Skrenta, un élève de 9e année. Ce virus ciblait les ordinateurs Apple II et se propageait par l'entremise de disquettes infectées. Pour en savoir davantage sur les programmes informatiques malveillants, voir Nicholas Weaver, « A Brief History of the Worm », *Security Focus*, 26 novembre 2001; Eugene Spafford, *The Internet Worm Program: An Analysis*, Purdue Technical Report CSD-TR-823, Département d'informatique, Purdue University, 8 décembre 1988.

7. Voir « White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 », 22 mai 1998.

8. Voir « The GAO Review of the NIPC », témoignage de Ronald L. Dick, directeur, National Infrastructure Protection Center, FBI, devant le Comité sénatorial américain de la justice, Sous-comité chargé du terrorisme, de la technologie et des renseignements du gouvernement, 22 mai 2001.

9. Voir General Accounting Office, « Critical Infrastructure Protection. 'ILOVEYOU' Computer Virus Highlights Need for Improved Alert and Coordination Capabilities », témoignage devant le Comité sénatorial américain des banques, du logement et des affaires urbaines, Sous-comité des institutions financières, 18 mai 2000.

10. Dans son témoignage devant un sous-comité sénatorial américain, le directeur du NIPC, Ronald Dick, a attribué cette lacune analytique à la réticence du département de la Défense et de la National Security Agency à détacher du personnel au Centre. Voir Dick, « The GAO Review of the NIPC » (2001).

11. La CNCI a été rendue publique en 2007, mais n'a été créée officiellement qu'en janvier 2008, lorsque le président Bush a signé la Directive présidentielle sur la sécurité nationale 54 / Directive présidentielle sur la sécurité intérieure 23. Une version non classifiée a été publiée le 2 mars 2010. Voir The White House, « The Comprehensive National Cybersecurity Initiative », *National Security Council*.

12. Voir Gouvernement des États-Unis d'Amérique, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 29 mai 2009, p. 4, [traduction].

13. Voir *Quadrennial Defense Review Report*, département de la Défense des États-Unis, 1er février 2010, p. 38. On signale aussi des cas où l'armée américaine a déjà été autorisée à attaquer des réseaux informatiques. Voir Shane Harris, « The Cyberwar Plan: It's not just a defensive game; cyber-security includes attack plans too, and the U.S. has already used some of them successfully », *National Journal*, 14 novembre 2009.

14. « L'exploitation non autorisée de réseaux informatiques » signifie entrer de force dans des systèmes et des réseaux informatiques afin d'en extraire les données sans les modifier. Dans une « attaque de réseaux informatiques », par ailleurs, on cherche intentionnellement à disloquer, à dégrader ou à détruire des ordinateurs ou des réseaux informatiques ennemis ou l'information qui y réside, ou à en interdire l'accès. Voir Mélanie Bernier et Joanne Truerniet, *CF Cyber Operations in the Future Cyber Environment Concept*, ministère de la Défense nationale, Recherche et développement pour la défense Canada, Direction d'analyse et de recherche opérationnelle, DRDC CORA TM 2009-058, décembre 2009, p. 7.

15. Thornburgh (2005).

16. « Remarks at the Defense Information Technology Acquisition Summit », allocution du secrétaire adjoint à la Défense William J. Lynn, III, Grand Hyatt, Washington (D.C.), 12 novembre 2009.

17. Une signature d'attaque est une mesure ou une série de mesures indiquant une tentative d'exploitation d'une vulnérabilité.

18. Ellen Nakashima, « Cybersecurity Plan to Involve NSA, Telecoms », *Washington Post*, 3 juillet 2009.

19. Gouvernement des États-Unis d'Amérique, *Cyberspace Policy Review* (2009).

20. Le 22 décembre 2009, pour faire preuve de « leadership aux plus hauts échelons » et faire avancer ces mesures et d'autres mesures à moyen terme, M. Obama a nommé Howard Schmidt, ex-dirigeant d'eBay et de Microsoft, coordonnateur de la cybersécurité. M. Schmidt fera rapport régulièrement au président et sera un membre clé de son National Security Council. « Introducing the New Cybersecurity Coordinator », *The White House Blog*, 22 décembre 2009.

21. Voir Conseil de l'Europe, *Convention sur la cybercriminalité*; la Convention est entrée en vigueur le 1er août 2004. Le 29 septembre 2006, les États-Unis ont déposé leur instrument de ratification de ce traité, tandis que le Canada en demeure seulement signataire. On trouvera dans Conseil de l'Europe, « Que voulez-connaître sur ce traité? », *Convention sur la cybercriminalité*, la liste de signatures et de ratifications.

22. À ce sujet, il convient de souligner que Google aurait demandé à la NSA de l'aider à se défendre contre de futures attaques. Selon les médias, leur collaboration ne visera pas à tenter de déterminer qui était responsable de l'attaque, parce que cela est « quasi impossible ». Ellen Nakashima, « Google to enlist NSA to help it ward off cyberattacks », *Washington Post*, 4 février 2010.

23. Par exemple, le président Obama a été critiqué pour avoir autorisé la NSA à continuer à participer au système Einstein de détection et de prévention des intrusions. Voir Jesselyn Radack, « NSA's cyber overkill », *Los Angeles Times*, 14 juillet 2009. L'Office of the General Legal Counsel a conclu qu'Einstein ne contrevenait pas aux lois sur l'écoute téléphonique et la confidentialité des communications. Voir Memorandum Opinion for an Associate Deputy Attorney General, « Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch », département de la Justice des États-Unis, 14 août 2009.

24. Chacun des pays partenaires des Five Eyes a fait allusion en public à son recours à l'exploitation non autorisée de réseaux informatiques afin de recueillir des renseignements touchant l'étranger. Par exemple, en 2007, devant le Comité sénatorial permanent de la sécurité nationale et de la défense du Canada, John Adams, chef du Centre de la sécurité des télécommunications du Canada (CSTC), a affirmé que son organisation avait le même objectif que son homologue américain, à savoir « maîtriser l'Internet », et a attiré l'attention du Comité sur le nombre croissant d'internautes en Afrique et au Proche-Orient. Expliquant pourquoi, en 2001, on a élargi le mandat de collecte de renseignements touchant l'étranger du CSTC afin de permettre la collecte de communications étrangères en partance ou à destination du Canada, M. Adams a noté : « Le problème des communications aujourd'hui est qu'il ne s'agit pas de service fixe. Avec Internet, nous ne pouvons pas savoir à tout moment qui parle avec qui. Nous visons les étrangers, mais nous ne saurons pas forcément s'ils discutent avec des étrangers. Lorsqu'Internet est devenu le mode de communication privilégié, nous avons en définitive été bâillonnés, car nous ne pouvions pas viser un étranger du fait que nous ne savions pas s'il n'allait pas s'entretenir avec un Canadien. On nous a damé le pion. » Comité sénatorial permanent de la sécurité nationale et de la défense, *Témoignages*, 1re session, 39e législature.

25. Pour consulter les stratégies des trois gouvernements, voir Royaume-Uni, Bureau du Cabinet, *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*, juin 2009; Australie, *Cyber Security*; et Nouvelle-Zélande, Ministère du Développement économique, *Digital Strategy 2.0*.

26. Karen Fournier, « Feds working on a broad national digital strategy; could be released in budget, experts say », *The Wire Report*, 25 janvier 2010.

27. Michael Wines, « China Issues Sharp Rebuke to U.S. Calls for an Investigation on Google Attacks », *New York Times*, 25 janvier 2010.

28. En juin 2009, les États-Unis ont établi un cybercommandement et se penchent actuellement sur la stratégie et la politique afin de mettre au point une approche globale de l'exploitation non autorisée des réseaux informatiques. Cependant, l'attaque de réseaux informatiques demeure pour certains de leurs alliés une activité litigieuse. Voir Jason Sherman, « Defense Department Launches Cyber Strategy and Policy Review », *Inside the Pentagon*, vol. 26, n° 1, 7 janvier 2010. Cette analyse d'Andrew Rathmell de la façon de penser aux États-Unis et en Europe au sujet de l'exploitation non autorisée de réseaux informatiques, bien que rédigée en 2001, n'en est pas moins perspicace. Voir Andrew Rathmell, « Controlling Computer Network Operations », *Information & Security*, vol. 7, 2001. Pour un examen plus récent de l'actuelle discussion de la doctrine au sein des Forces canadiennes, voir Bernier et Truerniet (2009).

29. Voir, par exemple, Ian Macleod, « U.S. plans to secure power grid worry producers », *Ottawa Citizen*, 22 novembre 2009.