



BIBLIOTHÈQUE *du* PARLEMENT

LIBRARY *of* PARLIAMENT

## ÉTUDE GÉNÉRALE



# Cybersécurité : défis techniques et stratégiques

Publication n° 2018-05-F  
Le 16 février 2018

**Holly Porteous**

Division des affaires juridiques et sociales  
Service d'information et de recherche parlementaires

Les **études générales** de la Bibliothèque du Parlement sont des analyses approfondies de questions stratégiques. Elles présentent notamment le contexte historique, des informations à jour et des références, et abordent souvent les questions avant même qu'elles deviennent actuelles. Les études générales 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, et ce, de façon objective et impartiale.

© Bibliothèque du Parlement, Ottawa, Canada, 2018

*Cybersécurité : défis techniques et stratégiques*  
(Étude générale)

Publication n° 2018-05-F

This publication is also available in English.

## TABLE DES MATIÈRES

1	CONTEXTE.....	1
2	ÉVOLUTION DES CYBERMENACES.....	1
2.1	Attaques visant des infrastructures essentielles .....	1
2.2	Attaques sur commande .....	2
2.3	Attaques visant à influencer l'opinion publique .....	2
2.4	Attaques visant les droits de la personne .....	3
3	CYBERSÉCURITÉ : PROBLÈMES ET SOLUTIONS.....	3
3.1	Qu'est-ce que la cybersécurité? .....	3
3.2	Défis de la cybersécurité.....	4
3.2.1	Pourquoi est-il si difficile d'assurer la cybersécurité? .....	4
3.2.2	Failles dans la sécurité de la cyberchaîne d'approvisionnement .....	7
3.2.3	Le dilemme de la cybersécurité.....	7
3.2.4	Devenir invisible .....	9
3.3	Solutions proposées en matière de cybersécurité .....	10
3.3.1	Peut-on changer Internet? .....	10
3.3.2	Gouvernance d'Internet.....	11
3.3.3	Groupe d'experts gouvernementaux des Nations Unies chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.....	12
3.3.4	Manuel de Tallinn 2.0 sur le droit international applicable aux cyberopérations.....	13
4	OBSERVATIONS ET CONCLUSIONS.....	14



# CYBERSÉCURITÉ : DÉFIS TECHNIQUES ET STRATÉGIQUES

---

## 1 CONTEXTE

Après un survol rapide de certains types de cybermenaces auxquels sont confrontés le Canada et ses alliés, la présente étude expose la manière dont le Canada définit la cybersécurité, ainsi que les nombreux facteurs humains, techniques, financiers et politiques qui expliquent pourquoi il est si difficile de garantir la cybersécurité. Elle décrit enfin certaines des initiatives internationales destinées à améliorer la cybersécurité.

## 2 ÉVOLUTION DES CYBERMENACES

Les cyberévénements récents suivants, survenus à l'étranger et au Canada, illustrent bien les formes que prennent les cybermenaces actuellement.

### 2.1 ATTAQUES VISANT DES INFRASTRUCTURES ESSENTIELLES

Le 23 décembre 2015, en Ukraine, les postes d'au moins trois grandes compagnies d'électricité ont été systématiquement attaqués, causant des interruptions temporaires de service qui ont privé d'électricité près d'un quart de million d'abonnés. Des analyses ont permis de déterminer par la suite que tous les ordinateurs utilisés pour mener cette attaque semblaient être situés sur le territoire de la Fédération de Russie. De manière non officielle, on a imputé l'attaque à un groupe de pirates informatiques russes connu sous le nom de « Sandworm » (du nom d'une créature des romans de science-fiction du cycle de *Dune*, de Frank Herbert; le code de logiciel des outils utilisés par ce groupe pour perpétrer les attaques contenait des références aux planètes fictives décrites dans ces romans)<sup>1</sup>.

Le 18 décembre 2016, soit un peu moins d'un an plus tard, le réseau électrique ukrainien a été de nouveau la cible d'une attaque. Cette fois, ce n'étaient pas les postes situés en aval dans la chaîne de distribution qui étaient visés, mais un important poste de transport d'électricité situé à Kiev. Même si la panne a duré moins longtemps que la fois précédente, le message était clair : les pirates contrôlaient le réseau électrique ukrainien et pouvaient le paralyser quand bon leur semblait<sup>2</sup>.

Le 12 mai 2017, le rançongiciel auto-répliquant dit « WannaCry » est apparu de manière fracassante, s'infiltrant dans des réseaux informatiques dans quelque 150 pays. Ce logiciel malveillant crypte les fichiers des ordinateurs ciblés, les rendant inutilisables jusqu'au versement d'une rançon au pirate, habituellement en bitcoins. Au moins 16 hôpitaux britanniques, le plus grand fournisseur de services de télécommunications espagnol, Telefónica, et la Fedex Corporation des États-Unis figurent au nombre des organisations infectées par WannaCry. Bien que, selon les médias, quelque 300 000 systèmes aient été touchés dans le monde, au Canada, aucune entreprise ni organisation n'a reconnu publiquement avoir été infectée<sup>3</sup>. Il est

rare que l'on attribue une cyberattaque à un État, mais, fait notoire, en décembre 2017, le Royaume-Uni, les États-Unis, l'Australie, la Nouvelle-Zélande, le Canada et le Japon ont accusé formellement la Corée du Nord d'être derrière cette attaque<sup>4</sup>. En droit international, une telle affirmation a des conséquences importantes, en ce qui concerne la réponse et la responsabilité. Autrement dit, à moins d'avoir un fort degré de certitude quant à l'origine d'une cyberattaque, on ne peut accuser personne, et la légitimité de toute mesure de représailles peut être remise en question.

Le 27 juin 2017, des banques, des ministères, des médias et des compagnies d'électricité de l'Ukraine ont été la cible d'une variante du maliciel « Petya » utilisé dans l'attaque à grande échelle menée un mois plus tôt au moyen du rançongiciel « WannaCry ». On a pensé initialement que l'objectif de cette attaque, que certains avaient surnommée « NotPetya », était l'extorsion de fonds. Or, d'après les modifications apportées à l'outil Petya utilisé pour cette attaque, certains analystes ont conclu que le but était plutôt de causer le maximum de dommages à l'infrastructure en effaçant des disques durs<sup>5</sup>. Le 15 février 2018, les États-Unis et le Royaume-Uni ont attribué formellement l'attaque « NotPetya » à l'armée russe<sup>6</sup>.

## 2.2 ATTAQUES SUR COMMANDE

Le 8 août 2017, la police israélienne a arrêté deux adolescents soupçonnés d'être les administrateurs de la plateforme vDOS, qui était à ce moment-là l'une des plus rentables pour les services en ligne d'attaques sur commande. Pendant les quatre années que vDOS a été opérationnelle, des dizaines de milliers de clients y auraient eu recours pour commanditer plus de deux millions d'attaques par déni de service distribué (DDoS). DDoS s'appuie sur des réseaux clandestins de milliers d'ordinateurs piratés ou « zombies » pouvant être réquisitionnés pour attaquer les systèmes informatiques des victimes en les submergeant de requêtes<sup>7</sup>.

En mars 2014, Karim Baratov, un citoyen canadien originaire du Kazakhstan, a été arrêté à Ancaster, en Ontario, relativement au piratage monstre de Yahoo ayant permis d'accéder aux données des comptes de 500 millions d'utilisateurs. M. Baratov (qui a été extradé vers les États-Unis) et trois autres personnes font face à des accusations de complot, de piratage informatique et d'espionnage économique dans le cadre d'une opération de collecte de renseignements menée au profit du Service fédéral de sécurité (SFS) de la Russie<sup>8</sup>.

## 2.3 ATTAQUES VISANT À INFLUENCER L'OPINION PUBLIQUE

Dès 2015, des pirates informatiques travaillant pour le compte d'agences de renseignement de la Fédération de Russie ont réussi à infiltrer le réseau informatique du Comité national démocrate (DNC) des États-Unis dans le cadre de l'opération GRIZZLY STEPPE<sup>9</sup>, comme l'ont appelée les autorités américaines. Certains avancent que la publication des courriels piratés du DNC a favorisé l'accession à la présidence de Donald Trump lors de l'élection de 2016<sup>10</sup>.

Depuis au moins une dizaine d'années, des observateurs remarquent que la Russie s'efforce de miner la cohésion au sein de l'OTAN et l'appui du public à son égard au moyen d'une stratégie de propagande qui, selon les analystes de la RAND Corporation Christopher Paul et Miriam Matthews, consiste à orchestrer la diffusion d'un flot ininterrompu d'informations mensongères<sup>11</sup>. Ces dernières années, ce type d'opérations se seraient multipliées sur Internet, avec l'utilisation de blogues et des médias sociaux pour diffuser de fausses nouvelles et s'attaquer à ceux dont les points de vue vont à l'encontre des intérêts russes. On utiliserait notamment des « usines de trolls » – nom que l'on donne à de véritables armées de gens que l'on paie pour publier des commentaires favorables à la Russie sur de faux comptes de médias sociaux – et des réseaux de machines « zombies » capables de diffuser de la propagande à très grande échelle.

## **2.4 ATTAQUES VISANT LES DROITS DE LA PERSONNE**

Le 19 juin 2017, le Citizen Lab, un centre de recherche de l'Université de Toronto, a publié un rapport d'analyse sur une campagne menée au moyen d'un logiciel espion<sup>12</sup> contre des journalistes, des avocats ainsi que des défenseurs des droits de la personne et de la santé publique au Mexique. Selon le Citizen Lab, une entreprise israélienne appelée NSO Group aurait mené la campagne d'espionnage pour le compte de membres du gouvernement mexicain. Le Citizen Lab a signalé en outre que, parmi les journalistes et les membres de la société civile ciblés par des tentatives d'infection effectuées au moyen de liens du NSO Group et parmi leurs collègues, beaucoup avaient aussi fait l'objet d'autres formes de harcèlement et d'intimidation<sup>13</sup>.

Comme l'illustrent ces événements, la cybersécurité va beaucoup plus loin que la protection de la technologie contre les attaques en ligne. Elle touche également la protection des personnes et de la société contre les campagnes cybernétiques d'influence, d'extorsion, de surveillance et d'intimidation.

## **3 CYBERSÉCURITÉ : PROBLÈMES ET SOLUTIONS**

### **3.1 QU'EST-CE QUE LA CYBERSÉCURITÉ?**

Tout le monde ne s'entend pas sur ce qu'est la cybersécurité. Pour un administrateur de systèmes, cela signifie que les réseaux, les systèmes informatiques, les appareils mobiles et les données qu'ils contiennent sont adéquatement protégés contre les actions non autorisées<sup>14</sup>. Les militants des droits civiques définissent souvent la cybersécurité comme une protection contre la surveillance en ligne émanant du gouvernement ou de sociétés privées. Pour un État-nation, la cybersécurité a des connotations géopolitiques. Par exemple, des pays comme la Chine et la Russie se méfient beaucoup de l'absence de frontières dans Internet et pour eux, la cybersécurité consiste à exercer un contrôle souverain sur les activités en ligne de leurs citoyens.

La Freedom Online Coalition, un groupe constitué de 30 gouvernements déterminés à travailler ensemble pour défendre la liberté sur Internet et protéger les droits fondamentaux de la personne, propose la définition suivante de la cybersécurité, rédigée avec la contribution du Canada :

Par cybersécurité, on entend la préservation – par des politiques, par la technologie et par l'éducation – de la disponibilité, de la confidentialité et de l'intégrité de l'information et de son infrastructure sous-jacente, dans le but d'accroître la sécurité des personnes à la fois en ligne et hors ligne<sup>15</sup>.

Le Canada soutient qu'il ne peut y avoir de compromis en matière de droits de la personne dans le contexte de la cybersécurité, estimant que les protections du droit international en la matière doivent s'appliquer dans le cyberspace<sup>16</sup>.

## 3.2 DÉFIS DE LA CYBERSÉCURITÉ

### 3.2.1 POURQUOI EST-IL SI DIFFICILE D'ASSURER LA CYBERSÉCURITÉ?

Si, comme le sous-entend la définition précitée, la cybersécurité repose essentiellement sur les personnes, les processus et la technologie, cela veut dire qu'il y a beaucoup d'impondérables. Les personnes – leur conscience des risques et leur respect des pratiques exemplaires en matière de sécurité susceptibles de minimiser ces risques – sont toujours les maillons faibles de n'importe quel système de sécurité. Trop souvent, soit les gens contournent les mesures de sécurité parce qu'elles sont contraignantes, soit ils font trop confiance à des mesures de sécurité insuffisantes. Une technologie mal conçue peut engendrer ces deux types de comportements.

D'autres facteurs viennent compliquer la cybersécurité, comme la rapidité de l'innovation technologique, les forces du marché et la concurrence géopolitique.

D'ailleurs, au-delà des considérations liées à l'interface utilisateur, les technologies de l'information et des communications (TIC), qui sont au cœur même du cyberspace, présentent des problèmes de sécurité quasi insurmontables. Les TIC sont particulièrement difficiles à protéger parce qu'elles reposent sur des logiciels<sup>17</sup>. Comme ces logiciels peuvent comprendre des millions de lignes de code et des sous-programmes obscurs, les possibilités d'erreurs sont grandes, les fonctionnalités risquent de ne pas être totalement comprises et on ne connaît pas toujours bien leur provenance. Si divers outils logiciels automatisés permettent de traquer les erreurs de codage et si les progrès de l'intelligence artificielle – particulièrement l'apprentissage machine – laissent entrevoir la possibilité qu'un jour cette intelligence sera utilisée pour appuyer le génie logiciel ou même prendre sa place, on s'en remet encore beaucoup aux compétences de codage et aux processus d'assurance de la qualité des humains<sup>18</sup>.

La forte concurrence – alimentée par la demande croissante des consommateurs<sup>19</sup> et par la mondialisation de l'innovation et de la production en matière de TIC – a rendu les cycles du marché de plus en plus serrés pour les produits des TIC. La Silicon Valley (tout comme ses homologues canadiens situés par exemple à Toronto, à Waterloo, à Vancouver, à Montréal et à Ottawa) est encore capable de générer



des innovations<sup>20</sup> mondiales stupéfiantes en matière de TIC, mais le vent commence à tourner. En effet, en juin 2017, par exemple, la Chine a franchi une étape importante dans le domaine de l'informatique quantique en réussissant à transmettre un signal quantique par satellite<sup>21</sup>.

Depuis 2000, le secteur des TIC de la région Asie-Pacifique est en pleine transformation. On ne se contente plus d'y faire l'assemblage de biens de consommation électroniques fabriqués ailleurs; l'innovation et la production locales progressent à grands pas. Aujourd'hui, le troisième fournisseur de téléphones intelligents en importance au monde est Huawei, une entreprise basée à Shenzhen, en Chine<sup>22</sup>. Huawei pourrait bientôt dépasser les compagnies qui occupent actuellement les première et deuxième places mondiales – la coréenne Samsung et l'américaine Apple –, mais seulement si elle réussit à conserver son avance sur deux autres concurrents chinois : Oppo et Vivo<sup>23</sup>.

Le service sans fil à large bande (et, de plus en plus, le câble à fibres optiques) a permis à des régions du globe mal desservies, comme l'Afrique, de se brancher, amenant sur le marché des millions de nouveaux consommateurs avides de technologies, pratiquement du jour au lendemain<sup>24</sup>. Grâce à des initiatives comme CSquared<sup>25</sup> et Project Loon<sup>26</sup>, de Google, au projet Aquila (Internet par drone)<sup>27</sup> de Facebook et au projet « Huit axes verticaux et huit axes horizontaux<sup>28</sup> », du fournisseur chinois de services de télécommunications China Communications Services Corporation, l'Afrique rejoint rapidement le reste du monde numérique. Comme c'est le cas ailleurs, ces nouveaux consommateurs qui, pour le moment, viennent essentiellement de centres urbains relativement cossus, ont intégré les appareils mobiles dans leur vie quotidienne, les utilisant pour visionner du contenu en ligne et communiquer avec leurs amis, leur famille et leur milieu de travail, pratiquement dès l'instant où ils se lèvent le matin. Même si, jusqu'à présent, seul un petit nombre d'entre eux se sert des appareils mobiles pour faire des transactions bancaires ou de petits achats, ils sont nombreux à avoir l'intention de faire ce genre d'opérations dès que l'offre de services le permettant sera largement répandue<sup>29</sup>. Pour les fournisseurs de TIC, le message est clair : pour tirer profit de la situation, il faut être le premier sur le marché à offrir des téléphones intelligents abordables et équipés de multiples fonctionnalités.

Somme toute, ce sont les logiciels – et non le matériel – qui permettent aux consommateurs d'obtenir les fonctions qu'ils veulent et aux fournisseurs de dégager les marges bénéficiaires qu'ils souhaitent<sup>30</sup>. De plus, comme le montre le modèle de numérisation de l'Afrique, les appareils mobiles remplacent rapidement les ordinateurs portables et les ordinateurs de bureau en s'imposant comme les technologies de choix<sup>31</sup>. Cette miniaturisation a des conséquences significatives sur le développement des logiciels. Contrairement aux logiciels fonctionnant sur des ordinateurs de bureau, les applications logicielles conçues pour les appareils mobiles, que l'on appelle couramment « applis », doivent être réduites de manière à tenir compte de contraintes comme la durée de vie de la pile et la petitesse des écrans.

Du point de vue de la sécurité, le fait que les applis soient épurées peut s'avérer une bonne chose, car le risque de faire des erreurs ou d'ajouter des fonctionnalités inutiles ou méconnues est limité. Quoi qu'il en soit, du fait qu'elles interagissent avec d'autres systèmes, les applis continuent d'exiger un codage rigoureux et bien documenté si l'on veut éviter des vulnérabilités en matière de sécurité<sup>32</sup>. Or, comme on s'empresse de répondre rapidement à la demande apparemment insatiable d'applications novatrices et faciles à utiliser, et qu'il y a beaucoup de codeurs qui soit ne savent pas écrire un code propre soit ont des intentions criminelles, les applications sécuritaires sont plus l'exception que la règle<sup>33</sup>. Il faut également garder à l'esprit que le matériel continue d'évoluer, tout comme la capacité des appareils mobiles à faire fonctionner des applications toujours plus sophistiquées, augmentant ainsi la probabilité d'avoir de mauvais codes, même si les fournisseurs passent les applications au crible pour y déceler des vulnérabilités.

Que ce soit pour des applications logicielles traditionnelles ou pour des applications destinées à des appareils mobiles, la conception de logiciels est devenue une vaste entreprise mondiale. Les possibilités d'introduction de failles de codage, que ce soit par inadvertance ou sciemment, sont très nombreuses. Par exemple, il est courant que des codeurs réutilisent des éléments de programmes offerts par des bibliothèques de codes sources ouverts gérées par des tiers, comme Github et Bitbucket. L'absence de vérification de codes de tiers réutilisés a provoqué des vulnérabilités majeures à grande échelle dans des caméras de surveillance d'aéroports, des capteurs, du matériel de réseautage et des dispositifs de l'Internet des objets<sup>34</sup>.

La production de puces de circuits intégrés est aussi devenue mondiale<sup>35</sup>. Jusqu'en 2005, la plupart des puces étaient fabriquées dans des fonderies de Taïwan<sup>36</sup>. Aujourd'hui, Taïwan demeure le premier producteur mondial, mais il se fait rattraper par la Corée du Sud; et la Chine a connu la plus forte augmentation globale sur le plan de la croissance de la capacité à ce chapitre<sup>37</sup>.

Bien sûr, même s'il était possible de rapatrier la totalité de la chaîne d'approvisionnement des TI<sup>38</sup>, des concurrents pourraient toujours suborner des employés et cibler certaines parties de la chaîne en utilisant des techniques comme l'hameçonnage pour rendre les systèmes vulnérables. Les alliés occidentaux, dont le Canada, sont parfaitement au fait des questions d'infiltration de la chaîne d'approvisionnement des TI. En 2006, par exemple, la National Security Agency (NSA) des États-Unis aurait – peut-être au su de son homologue canadien, le Centre de la sécurité des télécommunications (CST)<sup>39</sup> – payé un fournisseur américain bien connu de produits de cryptographie et l'Organisation internationale de normalisation afin qu'ils favorisent une méthodologie de chiffrement contenant une porte dérobée<sup>40</sup>. Encore plus loin dans le temps, en 1983, en Sibérie, une explosion spectaculaire a endommagé un gazoduc soviétique après qu'un logiciel contenant un maliciel intégré eut été remis au KGB dans le cadre d'une opération de déception menée par la CIA. Pendant des années, des agents du KGB s'étaient procuré illégalement de la technologie à l'Ouest; il s'agissait donc en quelque sorte d'un règlement de comptes<sup>41</sup>. Une entreprise canadienne aurait joué un rôle central dans l'acheminement de ce cheval de Troie jusqu'aux Soviétiques<sup>42</sup>.

### 3.2.2 FAILLES DANS LA SÉCURITÉ DE LA CYBERCHAÎNE D'APPROVISIONNEMENT

Au vu de ce qui précède, on ne doit pas s'étonner que la sécurité de la cyberchaîne d'approvisionnement<sup>43</sup> soit devenue une préoccupation de premier ordre, certains pays, comme les États-Unis, préconisant une interdiction complète de l'utilisation, dans les systèmes essentiels, de composants logiciels et matériels en provenance de pays présentant un risque pour la sécurité nationale, comme la Chine et la Russie<sup>44</sup>. Pour leur part, la Chine et la Russie semblent avoir imité les États-Unis en s'inspirant de certains aspects de leur politique. Le 1<sup>er</sup> juin 2017, par exemple, une nouvelle loi sur la cybersécurité est entrée en vigueur en Chine. Cette loi permet notamment au Centre chinois d'évaluation de la sécurité des technologies de l'information, qui relève du ministère de la Sécurité d'État, de demander leurs codes sources et autres biens relevant de la propriété intellectuelle aux fournisseurs de technologies exerçant des activités en Chine<sup>45</sup>.

Le 8 septembre 2017, le président russe Vladimir Poutine aurait affirmé, selon des médias, que les entreprises de technologie russes utilisant des logiciels d'origine étrangère susceptibles de représenter un risque pour la sécurité nationale pourraient perdre des marchés avec le gouvernement<sup>46</sup>. La Russie exige aussi des fournisseurs occidentaux de produits de sécurité des TI qu'ils lui remettent les codes sources de leurs produits, de manière que les laboratoires agréés par le Service fédéral de sécurité et le Service fédéral du contrôle technique et de l'exportation (un organisme du ministère de la Défense ayant notamment pour mandat de lutter contre le cyberespionnage) puissent les inspecter en vue découvrir les vulnérabilités exploitables et les portes dérobées éventuellement créées par des agences de renseignement<sup>47</sup>. Dans certains cas, la Russie permet la tenue de ces inspections des codes sources dans les installations protégées des fournisseurs<sup>48</sup>.

D'autres pays, comme le Canada et le Royaume-Uni, se sont aussi réservé le droit de tester formellement la fiabilité de ces types de produits d'origine étrangère avant de les utiliser<sup>49</sup>.

### 3.2.3 LE DILEMME DE LA CYBERSÉCURITÉ

Comme en témoigne l'augmentation des demandes d'inspection de produits de TI d'origine étrangère, pour y trouver des portes dérobées, il est difficile d'assurer la cybersécurité, mais nous y sommes pour quelque chose. Parfois, des vulnérabilités exploitables sont délibérément intégrées à des produits de TI à la demande d'organismes de sécurité nationale, et parfois elles sont tout simplement découvertes après la mise en marché du produit. Lorsqu'ils découvrent une importante faille ou en sont informés par des sources clandestines, les organismes de sécurité nationale gardent souvent le silence sur ce qu'ils savent, de manière à pouvoir utiliser la vulnérabilité pour recueillir des renseignements électromagnétiques dans le cadre de cyberopérations. Soit les fournisseurs ne sont pas au fait de ces prétendues vulnérabilités du « jour zéro », soit ils n'ont pas encore créé les correctifs nécessaires. En moyenne, il faut compter 6,9 ans pour que les personnes et les organisations se servant de ces dispositifs et réseaux vulnérables apprennent qu'elles sont susceptibles d'être visées par une attaque menée par des acteurs criminels ou étatiques<sup>50</sup>.

La communauté de la sécurité nationale rend cette façon de « garder le silence » par l'acronyme « NOBUS », pour « NObody But US » ou « personne d'autre que nous ». Le chercheur en cybersécurité Ben Buchanan croit que cette approche est devenue intenable<sup>51</sup>, car elle s'appuie sur la notion erronée que les États-Unis et ses partenaires du Groupe des cinq<sup>52</sup> peuvent conserver le monopole des connaissances sur les vulnérabilités de l'infrastructure mondiale de l'information et, grâce à ce monopole, contrôler la cybersécurité. Les documents divulgués par Edward Snowden, la mondialisation de la cyberchaîne d'approvisionnement, les initiatives visant à affirmer la souveraineté nationale sur l'infrastructure du cyberspace (dont il sera question plus loin en détail), sans compter celles des pays non alliés destinées à vérifier les codes sources des logiciels ne sont que quelques-unes des raisons expliquant pourquoi cette approche du « personne d'autre que nous » est intenable selon Buchanan et d'autres observateurs<sup>53</sup>. À bien des égards, cette approche revient à assurer la sécurité par l'obscurité, mais ce que l'on a déjà découvert et que l'on continue de découvrir ne lui permettra pas de continuer à fonctionner de manière prévisible.

Au lendemain des attaques perpétrées en mai 2017, au moyen des rançongiciels « WannaCry » et « Petya » utilisant les outils de cyberexploitation de la NSA qui ont fait l'objet de fuites et frappé les infrastructures essentielles de 65 pays, des voix se sont élevées contre la pratique du gouvernement d'exploiter une réserve de vulnérabilités du jour zéro<sup>54</sup>. Cela a fait réagir l'ancien directeur adjoint de la NSA, Rick Ledgett, à la retraite depuis peu, lequel estime que le fait de mettre fin à cette pratique de la NSA reviendrait à procéder à un désarmement unilatéral des États-Unis dans un secteur où ils ne peuvent pas se permettre de se retrouver désarmés<sup>55</sup>. Il a fait valoir qu'aucun des alliés et des adversaires des États-Unis n'abandonnerait les vulnérabilités en sa possession. Au demeurant, a-t-il ajouté, si les États-Unis renonçaient à exploiter ces vulnérabilités, cela induirait une crise de confiance chez leurs alliés, qui seraient enclins à douter de leur capacité à gérer des sources et des méthodes sensibles<sup>56</sup>.

Contrairement aux autres membres du Groupe des cinq, les États-Unis ont donné un aperçu du processus interorganisationnel qu'ils utilisent pour évaluer les risques relatifs que présente la divulgation ou la dissimulation de renseignements sur les vulnérabilités du jour zéro, soit le Vulnerabilities Equities Process (VEP). Par exemple, dans la foulée du scandale sur la vulnérabilité de sécurité Heartbleed<sup>57</sup>, en 2014, Michael Daniel, adjoint spécial du président américain et coordonnateur de la cybersécurité, a parlé du processus en détail dans un billet du blogue de la Maison-Blanche<sup>58</sup>. Pour sa part, le Canada est resté relativement muet sur la question<sup>59</sup>.

Le 17 mai 2017, un projet de loi visant à codifier le VEP a été déposé à la Chambre des représentants et au Sénat des États-Unis<sup>60</sup>. Fait important, ce projet de loi prévoit d'inclure dans le VEP une évaluation des risques que présente, pour les autres pays et leurs citoyens, le fait de ne pas communiquer ou diffuser des renseignements sur des vulnérabilités. Pour les alliés des États-Unis faisant partie du Groupe des cinq, dont le Canada, ces risques peuvent comprendre notamment celui de ne plus pouvoir utiliser une importante méthode de collecte de renseignements électromagnétiques qu'ils ont pourtant contribué à créer.

### 3.2.4 DEVENIR INVISIBLE

Le débat récurrent sur l'invisibilité et la prise de mesures de chiffrement rigoureuses suscite aussi un dilemme en matière de cybersécurité. On parle d'invisibilité quand une personne ciblée prend des mesures pour occulter ses communications et échapper ainsi à la surveillance des organismes d'application de la loi et de sécurité nationale. Pour dire les choses simplement, le travail des organismes d'application de la loi et de sécurité nationale est désormais beaucoup plus difficile, car les fournisseurs de services Internet et les citoyens sont plus nombreux à prendre la cybersécurité au sérieux. Par exemple, les principaux fournisseurs de services Internet ont commencé à offrir le chiffrement de bout en bout<sup>61</sup> après les divulgations d'Edward Snowden faites en 2013 sur le programme du Groupe des cinq appelé MUSCULAR. Ce programme permettait aux organismes de renseignement électromagnétique de contourner l'obligation d'obtenir un mandat pour collecter des renseignements auprès de fournisseurs de services Internet du secteur privé en accédant directement aux réseaux internationaux qu'utilisaient ces derniers pour transmettre les communications de leurs clients<sup>62</sup>. C'est pour regagner la confiance des consommateurs que les grands fournisseurs comme Google, Facebook et Apple ont commencé à offrir des applications de messagerie et de courriel chiffrés<sup>63</sup>.

Certains alliés du Canada soutiennent que ce chiffrement de bout en bout les empêche de détecter et de déjouer les complots terroristes. À la suite d'une réunion des ministres de la Sécurité publique, de l'Immigration et de la Justice du Groupe des cinq tenue à Ottawa, en juin 2017, le premier ministre de l'Australie Malcolm Turnbull a demandé aux entreprises de télécommunications d'interdire volontairement tous les systèmes permettant le chiffrement de bout en bout. De son côté, la ministre britannique de l'Intérieur, Amber Rudd, a fait valoir que les « gens ordinaires » n'ont pas besoin du chiffrement de bout en bout<sup>64</sup>. Au Canada, le commissaire de la Gendarmerie royale du Canada, Bob Paulson, a confié aux journalistes, en novembre 2016, que les organismes d'application de la loi ont besoin de recours judiciaires pour avoir accès à l'information chiffrée, car la technologie moderne est utilisée tous les jours pour faciliter des activités criminelles qui échappent aux forces policières<sup>65</sup>. Selon des médias, dans une note d'information du 23 juin 2016 adressée au conseiller à la sécurité nationale et au renseignement du Canada divulguée en vertu de la *Loi sur l'accès à l'information*, la Gendarmerie royale du Canada (GRC) estime être en retard par rapport à ses homologues du Groupe des cinq en ce qui a trait à ses capacités d'enquête numériques<sup>66</sup>.

Les contre-arguments à ces demandes visant à réduire le chiffrement viennent de sources surprenantes. Deux personnes qui étaient récemment à la tête d'organismes de renseignement électromagnétique – Michael Hayden et Robert Hannigan, respectivement ancien directeur de la NSA<sup>67</sup> et ancien directeur du Government Communications Headquarters du Royaume-Uni – se sont prononcés contre l'installation de portes dérobées dans les programmes de chiffrement, soutenant que les coûts globaux pour la cybersécurité seraient trop élevés. Les deux hommes croient qu'il vaudrait mieux que les organismes de sécurité nationale s'attaquent aux faiblesses des points terminaux – par exemple, aux pratiques sous-optimales des utilisateurs en matière de sécurité et aux vulnérabilités des logiciels tournant sur les appareils des utilisateurs<sup>68</sup> – plutôt qu'à l'algorithme de chiffrement même<sup>69</sup>.

### 3.3 SOLUTIONS PROPOSÉES EN MATIÈRE DE CYBERSÉCURITÉ

#### 3.3.1 PEUT-ON CHANGER INTERNET?

Maintenant, la plupart des gens savent qu'ils s'exposent à des risques chaque fois qu'ils vont sur Internet pour faire des transactions bancaires et des achats ou envoyer un message. Peu savent que le problème réside dans la façon dont Internet a été conçu, puisque l'impératif premier d'Internet était la survie, et non la sécurité. Le protocole de contrôle de transmission/protocole Internet (protocole TCP/IP) – qui est la norme technique sous-tendant Internet – a été créé à une époque où l'on craignait la destruction partielle du réseau par des armes nucléaires. Le protocole TCP/IP veille donc à ce que l'information soit acheminée là où l'on en a besoin en la divisant en plusieurs paquets de données et en utilisant ensuite n'importe quelle voie d'acheminement viable pour la livraison de ces paquets de données à leur destination finale, où ils sont réassemblés.

Dans l'architecture TCP/IP, l'accent est mis sur la connectivité et non sur le contenu – les protocoles TCP/IP permettent la livraison fiable de paquets de données sans égard à ce qui est envoyé. C'est ainsi que, depuis presque les tout débuts, des acteurs malveillants exploitent l'aveuglement d'Internet au contenu en envoyant des paquets de données auxquels sont intégrés des éléments nuisibles ou simplement en ouvrant les « vannes » de livraison des paquets au cours d'attaques par déni de service distribué (DDoS). La criminalité en ligne a progressé en même temps que la connectivité est devenue omniprésente et continue. Selon certaines estimations, le coût de la cybercriminalité pour l'économie mondiale atteindra 6 billions de dollars en 2021<sup>70</sup>.

Cela peut paraître surprenant, mais la technologie permettant d'éliminer la plupart des formes de malveillance en ligne existe et est utilisée depuis près d'une vingtaine d'années. On doit l'invention de cette technologie, appelée système Handle<sup>71</sup>, à Robert Kahn, l'Américain qui a inventé le protocole TCP/IP avec Vinton Cerf, un autre Américain<sup>72</sup>. Essentiellement, le système Handle n'est plus axé sur l'acheminement de paquets de données anonymes. Il offre une nouvelle vision d'Internet, qui consiste en une énorme base de données où l'accent est mis sur l'accès à des « objets numériques », comme des pages Web, des documents de recherche ou des appareils branchés à Internet.

Dans le système de M. Kahn, les objets numériques se voient attribuer des identifiants permanents qu'on appelle *handles*. Les *handles* fournissent des métadonnées sur les objets numériques, notamment les endroits où ils se trouvent, leurs formats, les personnes autorisées à y avoir accès et tout paiement nécessaire pour les obtenir. Dans un souci de respect de la vie privée, les personnes souhaitant avoir accès à une ressource doivent pouvoir conserver un certain anonymat au moyen d'une identité d'utilisateur créée pour ce seul service. Les bibliothèques et les établissements d'enseignement ont été parmi les premiers à adopter ce système et à utiliser des *handles* pour identifier et gérer l'accès aux ressources documentaires en leur possession<sup>73</sup>.

Du point de vue de la sécurité, l'identification des objets numériques est attrayante, car elle permet un contrôle plus important et plus précis des ressources branchées à Internet. Le système Handle fait naître l'espoir qu'à mesure que le nombre d'appareils branchés à l'Internet des objets (IdO) augmentera, ces objets branchés comme des poupées, des réfrigérateurs et des aquariums<sup>74</sup> ne pourront pas être utilisés contre nous.

Bien entendu, les identifiants uniques peuvent aussi s'appliquer aux personnes, ce qui ouvre la porte à une plus grande surveillance de leur vie en ligne et hors ligne. Ce n'est pas une coïncidence si la Chine, la Russie et l'Arabie saoudite sont toutes d'ardents partisans de la mise en œuvre d'un système Handle appelé architecture d'objet numérique (AON). Chacun de ces pays a été critiqué par des groupes de défense des droits de la personne pour leur ligne dure à l'égard des libertés civiles<sup>75</sup>. La Chine et la Russie ont depuis longtemps fait comprendre que, pour elles, le but de la cybersécurité consiste à protéger l'*information* et non pas les *systèmes*<sup>76</sup>. Lors de l'Assemblée mondiale de normalisation des télécommunications (AMNT) de l'Union internationale des télécommunications (UIT) des Nations Unies<sup>77</sup> organisée en Tunisie en novembre 2016, elles faisaient partie des pays ayant exercé de fortes pressions, par l'intermédiaire d'une série de résolutions, pour que l'UIT intègre l'AON dans ses travaux.

Soutenant que cela irait à l'encontre de la tradition de neutralité de l'UIT sur le plan de la technologie – l'AON étant une technologie exclusive et le Global Handle System étant géré par une société privée appelée DONA Foundation –, plusieurs pays (dont le Canada) avec à leur tête les États-Unis ont réussi à faire rejeter chacune des six résolutions sur l'intégration de l'AON<sup>78</sup>. Ce n'est pas la première fois que l'UIT sert de champ de bataille pour le contrôle d'Internet et ce ne sera probablement pas la dernière.

### 3.3.2 GOUVERNANCE D'INTERNET

En 2015, à la dixième Conférence de plénipotentiaires de l'UIT organisée à Guadalajara, au Mexique, la Russie et un groupe d'anciens pays du bloc soviétique ont proposé que l'UIT prenne en charge le travail du Comité consultatif gouvernemental (GAC) de la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN). L'ICANN est une organisation internationale à but non lucratif chargée de coordonner l'attribution de l'espace des adresses IP, les noms de domaine<sup>79</sup> de premier niveau et d'autres éléments techniques permettant à Internet de fonctionner. Essentiellement, l'ICANN administre le « carnet d'adresses » d'Internet<sup>80</sup>. Conformément au modèle multilatéral fondé sur le consensus de l'ICANN, le GAC n'est qu'une entité parmi d'autres qui contribue au travail de l'ICANN. Au nombre des autres intervenants de l'ICANN figurent des entreprises du secteur privé, des experts techniques, des universitaires, des organisations de la société civile et des membres du public.

La Russie n'a pas gagné son pari de transférer la responsabilité du travail du GAC à l'UIT, mais si elle avait réussi, les changements à la gouvernance d'Internet auraient été profonds. Le fonctionnement de l'UIT repose sur le principe « un pays, une voix ». C'est pour cette raison que le Canada et ses alliés ont tout fait pour que les

questions liées à la gouvernance d'Internet et à la cybersécurité ne relèvent pas de l'UIT. Quand on constate qu'un groupe de régimes autoritaires a réussi à faire du système Handle l'approche *de facto* en matière de gestion de l'identité dans l'IdO, force est de conclure que de confier la prise de décisions ayant des répercussions sur la cybersécurité uniquement aux États pourrait avoir de graves conséquences pour la liberté sur Internet. Mis en œuvre sans égard à ses répercussions sur les droits de la personne, le système Handle et, d'ailleurs, toute technologie reposant sur l'attribution permanente d'identifiants uniques à des appareils et à des personnes<sup>81</sup> constitue une façon idéale pour les régimes autoritaires de verrouiller leur partie d'Internet.

### 3.3.3 GROUPE D'EXPERTS GOUVERNEMENTAUX DES NATIONS UNIES CHARGÉ D'EXAMINER LES PROGRÈS DE L'INFORMATIQUE ET DES TÉLÉCOMMUNICATIONS DANS LE CONTEXTE DE LA SÉCURITÉ INTERNATIONALE

Jusqu'à tout récemment, il y avait lieu de croire qu'un consensus international finirait par se dégager sur la conduite des États dans le cyberspace. Le Groupe d'experts gouvernementaux des Nations Unies chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale s'emploie à examiner les normes de comportement dans le cyberspace depuis sa création, en 2004. Le Canada en a été membre en 2012-2013 et en 2016-2017.

On doit au Groupe d'experts gouvernementaux des Nations Unies l'établissement du programme mondial sur la cybersécurité et la promotion de la norme voulant que le droit international s'applique au comportement des États dans le cyberspace<sup>82</sup>. Bien qu'ils ne soient pas juridiquement contraignants, les rapports du Groupe d'experts gouvernementaux servent à définir les normes de comportement et à appuyer les mesures de renforcement de la confiance et des capacités. Par exemple, en 2015, les membres du Groupe ont convenu :

[qu'un] État ne devrait pas mener ou soutenir sciemment une activité informatique qui est contraire aux obligations qu'il a contractées en vertu du droit international et qui endommage intentionnellement une infrastructure essentielle ou qui compromet l'utilisation et le fonctionnement d'une infrastructure essentielle pour fournir des services au public<sup>83</sup>.

Or, lors de sa plus récente réunion, qui s'est déroulée du 19 au 23 juin 2017, le Groupe d'experts n'est pas parvenu à un consensus sur les solutions qui devraient s'offrir aux pays pour réagir à des cyberattaques ni sur le rôle que les Nations Unies doivent jouer, le cas échéant, dans l'imposition de sanctions contre les auteurs des cyberattaques. Certains croient que l'incapacité des membres du Groupe de s'entendre sur ces questions clés et le fait que des attaques contre des infrastructures essentielles continuent de se produire en contravention des normes convenues remettent en question l'avenir du Groupe<sup>84</sup>. À tout le moins, l'impasse dans laquelle se trouve ce dernier révèle que bon nombre de questions fondamentales sur les cyberactivités ne sont toujours pas réglées.



La Chine fait partie des pays refusant de discuter de la façon dont le droit international actuel devrait s'appliquer dans le cyberspace. De concert avec la Russie, elle affirme depuis quelque temps que les pays devraient travailler à l'élaboration d'un traité, par l'intermédiaire du système des Nations Unies, plutôt que discuter de la façon de réglementer la guerre cybernétique au moyen du droit international actuel. À cet égard, la Chine, la Russie, le Kazakhstan, le Kirghizistan, l'Ouzbékistan et le Tadjikistan ont proposé à de multiples reprises un projet de code de conduite international sur la sécurité de l'information qu'ils ont conçu en 2011. Une version révisée de ce projet de code a été présentée au secrétaire général des Nations Unies en 2015<sup>85</sup>, deux ans après que la Chine eut indiqué, dans le rapport consensuel du Groupe d'experts gouvernementaux de 2012-2013, qu'elle acceptait l'application du droit international – y compris la *Charte des Nations Unies*<sup>86</sup> – dans le cyberspace<sup>87</sup>.

Dans un document daté du 17 août 2017, le juriste américain Julian Ku examine l'interprétation que fait la Chine du *jus ad bellum*, ou droit de faire la guerre – c'est-à-dire les conditions dans lesquelles un État peut entrer en guerre ou employer une force armée – et les retombées éventuelles de cette interprétation sur la manière dont la Chine aborde la guerre cybernétique<sup>88</sup>. Bien que, conformément au sens qu'elle donne au *jus ad bellum* – tel qu'il est codifié dans la *Charte des Nations Unies* –, la Chine accepte le recours à la force en cas d'attaque armée, M. Ku fait observer qu'elle a une vision beaucoup plus étroite que les États-Unis quant aux circonstances dans lesquelles un État peut légitimement recourir à la force et aux circonstances dans lesquelles il peut invoquer la légitime défense. Essentiellement, dit M. Ku, la Chine estime que toutes les décisions relatives au recours à la force doivent être approuvées par le Conseil de sécurité des Nations Unies, sauf en situation de légitime défense. M. Ku ajoute que :

Les universitaires chinois se montrent tous sceptiques à l'égard du droit à la légitime défense avant même la perpétration d'une attaque armée. Bien qu'ils respectent le critère de l'« imminence » fondé sur la célèbre affaire du *Caroline*<sup>89</sup>, ils n'admettent aucune définition vague ou large de ce critère<sup>90</sup>.

Ainsi, dit M. Ku, dans l'interprétation que fait la Chine du *jus ad bellum*, le simple fait de planifier une attaque armée ne peut pas être considéré comme une attaque armée appelant des mesures de légitime défense.

### 3.3.4 MANUEL DE TALLINN 2.0 SUR LE DROIT INTERNATIONAL APPLICABLE AUX CYBEROPÉRATIONS

Contrairement à la Chine, les États-Unis (et probablement ses proches alliés, comme le Canada<sup>91</sup>) semblent estimer qu'il existe des circonstances dans lesquelles la prise de mesures de légitime défense préventive bien avant qu'une cyberattaque se mue en attaque armée pourrait être justifiée. Ces circonstances sont décrites dans la règle 73 du Manuel de Tallinn 2.0 sur le droit international applicable aux cyberopérations (*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*).

La deuxième version du Manuel de Tallinn consiste en un examen non contraignant, mais faisant autorité, de l'application du droit international aux cyberopérations. Sous

la direction du juriste américain Michael Schmitt, sa rédaction a été confiée à un groupe multinational d'experts du droit international venant principalement, mais pas exclusivement, des pays membres de l'OTAN. Le Canada a participé à la rédaction des deux versions du manuel. La Chine a aussi contribué à son ébauche<sup>92</sup>, mais des médias et des universitaires chinois ont exprimé un grand scepticisme à l'égard de sa version définitive, si l'on en croit M. Ku<sup>93</sup>.

Bien que la règle 73 du manuel de Tallinn reconnaisse que la légitime défense préventive ne fait pas l'unanimité, on y précise que la majorité des membres du groupe d'experts international responsable de la rédaction du manuel ont rejeté l'analyse temporelle stricte comme norme au profit du principe du dernier moment propice. Selon la règle 73, ce moment propice peut survenir immédiatement avant l'attaque en question ou, dans certains cas, bien avant qu'elle se produise<sup>94</sup>. Toutefois, le manuel de Tallinn fait aussi observer que selon la majorité des membres, le principe du dernier moment propice ne soustrait pas complètement les États au respect de la norme temporelle. Selon eux, moins une attaque est imminente, plus grande est la probabilité que d'autres solutions d'intervention soient envisageables.

## 4 OBSERVATIONS ET CONCLUSIONS

Comme on vient de le voir, la cybersécurité est une question complexe et multidimensionnelle qui intéresse de nombreux acteurs. Les solutions techniques sont à la fois prometteuses et périlleuses. Des protocoles rigoureux de chiffrement et de protection de la vie privée permettent aux citoyens de commercer et de converser sans crainte. Cependant, ces mêmes protections favorisent aussi la criminalité et compliquent grandement le travail des organismes de sécurité nationale et d'application de la loi.

L'apparente tendance croissante des États à vouloir inspecter les codes sources des produits de TI avant leur lancement conjuguée au perfectionnement continu des outils d'inspection des codes donne des pistes de solution pour rétablir la confiance. Le fait de savoir qu'il y a de fortes chances que des inspections permettent la découverte de vulnérabilités et de portes dérobées ne peut qu'inciter les concepteurs à fabriquer correctement les produits dès le départ. Le défi consistera à multiplier les essais techniques et les tests d'assurance de la qualité rigoureux sur les systèmes et les réseaux. Ce n'est pas une mission impossible, mais ce sera difficile<sup>95</sup>.

Les solutions stratégiques, en particulier celles concernant la gouvernance d'Internet et les cybernormes, présentent des perspectives d'avenir nettement différentes. S'il était uniquement régi par les États, le cyberdomaine pourrait certainement être plus sûr, mais le Canada et ses alliés estiment que ce cela se ferait trop aux dépens des droits de la personne. Régi par une multitude d'acteurs différents travaillant au sein d'un nombre tout aussi grand de tribunes internationales, Internet est relativement libre et ouvert, mais rien ne garantit qu'il le restera. Des États comme la Russie et la Chine se sont déjà montrés déterminés à exercer un contrôle souverain sur leur cyberspace en adoptant des mesures comme la localisation des données stockées, le blocage de l'accès au contenu Internet et la réglementation de l'utilisation de réseaux privés virtuels.

## NOTES

1. Andy Greenberg, « [How an Entire Nation Became Russia's Test Lab for Cyberwar](#) », *Wired*, 20 juin 2017. « Dragonfly », l'agent de menace opérant depuis la Russie soupçonné d'être derrière les attaques contre l'Ukraine, a aussi été mis en cause dans une longue campagne d'activités de reconnaissance visant des infrastructures énergétiques européennes, américaines et canadiennes. Voir Kevin Poulsen, « [Russia-Linked Hackers Breached 100 Nuclear and Power Plants Just This Year](#) », *Daily Beast*, 6 septembre 2017.
2. Greenberg (2017).
3. Cependant, un hôpital d'Oshawa, en Ontario, a dit que son logiciel antivirus avait stoppé la tentative d'infection en bloquant un courriel reçu contenant le maliciel WannaCry. Voir Howard Solomon, « [WannaCry just a taste of NSA-charged cyber attacks to come](#) », *IT World Canada*, 15 mai 2017; et Nicole Thompson, « ['We were lucky': Massive 'WannaCry' cyberattack avoids Canada](#) », *Globe and Mail*, 13 mai 2017.
4. Howard Solomon, « [Canada helped confirm North Korea behind Wannacry ransomware, says U.S.](#) », *IT World Canada*, 19 décembre 2017.
5. Jacob Kastrenakes, « [Petya virus is something worse than ransomware, new analysis shows](#) », *The Verge*, 28 juin 2017. Voir aussi Alex Hern, « ['NotPetya' malware attacks could warrant retaliation, says Nato-affiliated researcher](#) », *The Guardian*, 3 juillet 2017.
6. « [UK and US blame Russia for 'malicious' NotPetya cyber-attack](#) », *BBC News*, 15 février 2018.
7. Brian Krebs, « [Alleged vDOS Operators Arrested, Charged](#) », *Krebs on Security* (blogue), 9 août 2017.
8. Cour de district des États-Unis pour le district nord de la Californie, [United States of America v. Dmitry Dokuchaev, aka "Patrick Nagel," Igor Sushchin, Alexsey Belan, aka "Magg," and Karim Baratov, aka "Kay," aka "Karim Taloverov," aka "Karim Ake Ahmet Tokbergenov"](#), 28 février 2017. Voir aussi Kevin Poulsen, « [Russian Spies' Hacker-for-Hire Pleads Not Guilty to Cracking Yahoo](#) », *Daily Beast*, 23 août 2017; Kelly Bennett, « [Karim Baratov, alleged Yahoo hacker, pleads not guilty in U.S. court](#) », *CBC News*, 23 août 2017; et « [Karim Baratov, the Canadian man accused in Yahoo hack, pleads guilty in American court](#) », *Toronto Star*, 28 novembre 2017.
9. États-Unis, Département de la Sécurité intérieure et Federal Bureau of Investigation, [GRIZZLY STEPPE – Russian Malicious Cyber Activity](#), Joint Analysis Report, JAR-16-20296A, 29 décembre 2016.
10. Voir Thomas Rid, « [How Russia pulled off the biggest election hack in U.S. history](#) », *Esquire*, 20 octobre 2016. Pour une analyse approfondie de la vaste campagne de mesures actives de la Russie, voir Garrett M. Graff, « [A Guide to Russia's High Tech Tool Box for Subverting U.S. Democracy](#) », *Wired*, 13 août 2017.
11. Voir Christopher Paul et Miriam Matthews, « [The Russian 'Firehose of Falsehood' Propaganda Model: Why it Might Work and Options to Counter It](#) », *Perspective*, RAND Corporation, 11 juillet 2016. Pour en apprendre davantage sur l'utilisation des zombies dans la diffusion de la propagande, voir [The Computational Propaganda Project](#), Oxford Internet Institute, Université d'Oxford.
12. Un logiciel espion est un programme installé secrètement sur un ordinateur ciblé afin de surveiller son utilisateur à son insu.
13. John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata et Ron Deibert, [Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware](#), The Citizen Lab, 19 juin 2017.

14. Ou, plus précisément, un administrateur de systèmes doit s'assurer de protéger la confidentialité, l'intégrité et la disponibilité des données et des systèmes.
15. Freedom Online Coalition, « Blog #8: Why do we need a new definition for cybersecurity? », série de blogues du groupe de travail 1 de la Freedom Online Coalition mise à jour en septembre 2015 et consultée le 20 janvier 2018 [TRADUCTION]. À noter que cette définition englobe les définitions ISO 27000 de « confidentialité, intégrité et disponibilité ». ISO, qui signifie « Organisation internationale de normalisation », est une organisation non gouvernementale indépendante dont le siège est basé à Genève, en Suisse.
16. Voir « Blog #10: Four common myths about human rights and security in cyberspace » (billet élaboré à partir des remarques de Michael Walma, coordinateur du cyberspace pour Affaires mondiales Canada, faites lors de l'atelier du groupe de travail 1 de la Freedom Online Coalition dont le thème était : « Une approche de cybersécurité multilatérale et centrée sur les droits de la personne », qui s'est tenu du 10 au 13 novembre 2015, dans le cadre du 10<sup>e</sup> Forum annuel sur la gouvernance d'Internet, à João Pessoa, au Brésil), série de blogues du groupe de travail 1 de la Freedom Online Coalition consultée le 20 janvier 2018.
17. Même si certains cyberexploits – comme les attaques par canaux auxiliaires permettant d'analyser l'énergie consommée afin de recueillir de l'information sur la clé de chiffrement utilisée pour protéger les données sur un ordinateur – sont rendus possibles grâce aux défauts du matériel ou des micrologiciels utilisés pour monter les ordinateurs et les réseaux informatiques, la plupart des attaques réussies visent des logiciels mal conçus et non testés adéquatement. Des experts en sécurité ont mentionné toutefois deux cybervulnérabilités décelées récemment et surnommées « Spectre » et « Meltdown » pour illustrer la menace grandissante posée par les défauts de conception au niveau des microprocesseurs. Voir Bruce Schneier, « [The Effects of the Spectre and Meltdown Vulnerabilities](#) », *Schneier on Security* (blogue), 26 janvier 2018.
18. Voir, par exemple, Esther Shein, « [How AI is Changing Software Development](#) », *Communications of the ACM*, 26 janvier 2017.
19. Les tendances actuelles indiquent que les abonnements à la large bande augmentent de 20 % par année, et c'est en Chine que la progression est la plus forte. Pour en apprendre davantage sur les tendances internationales concernant les TIC, voir Union internationale des télécommunications (UIT) des Nations Unies, [ICT Facts and Figures 2017](#) [DISPONIBLE EN ANGLAIS SEULEMENT].
20. Par exemple, D-Wave Systems, une entreprise de Burnaby, en Colombie-Britannique, est la première et plus importante société d'informatique quantique au monde. Google a fait l'acquisition de tous les systèmes que D-Wave a produits jusqu'à présent, et a conclu un marché de plusieurs années avec la compagnie pour lui acheter chacun des nouveaux systèmes qu'elle créera. Pour en savoir plus sur l'informatique quantique et D-Wave, écouter Rob Reid, [Quantum computing's terrifying promise](#), fichier balado diffusé sur *Boing Boing* (blogue), 6 septembre 2017.
21. Davide Castelvecchi, « [China's quantum satellite clears major hurdle on way to ultrasecure communications](#) », *Nature*, 15 juin 2017. Lorsqu'elle deviendra viable, l'informatique quantique aura une incidence majeure sur un aspect de la cybersécurité : le chiffrement. Premièrement, avec l'énorme capacité de traitement des ordinateurs quantiques, ce sera un jeu d'enfant que d'arriver à percer le code de la plupart des clés de chiffrement existantes (voire de toutes), qui s'appuient sur des algorithmes reposant sur des calculs complexes. Deuxièmement, comme elle se fonde sur la physique et non les mathématiques, la cryptographie quantique devrait ouvrir la voie à une nouvelle ère de chiffrement impénétrable.
22. Saheli Roy Choudhury, « [Chinese tech giant Huawei sees 15% revenue jump in first half](#) », *CNBC*, 27 juillet 2017.

23. « [Huawei narrows gap with Samsung, Apple in smartphone sales: Gartner](#) », *Reuters*, 23 mai 2017.
24. Steve Song, [Unlocking Affordable Access in Sub-Saharan Africa](#), Global Commission on Internet Governance, Paper Series n° 43, Centre for International Governance Innovation et Chatham House, novembre 2016.
25. Site Web de [CSquared](#).
26. Site Web de [Project Loon](#).
27. Mark Zuckerberg, « [The technology behind Aquila](#) », *Facebook*, 21 juillet 2016.
28. Li Yan, « [Chinese company builds network to boost internet access in Africa](#) », *People's Daily Online*, 29 mars 2017 [TRADUCTION].
29. Deloitte, [Game of Phones: Deloitte's Mobile Consumer Survey: The Africa Cut 2015/2016](#), 30 août 2016, p. 32.
30. Selon Ralph Pini, chef de l'exploitation et directeur général, Appareils, chez BlackBerry, l'investissement dans la conception et la fabrication de matériel n'est rentable que lorsque le fournisseur est intégré verticalement et qu'il cherche à créer un « écosystème » qu'il contrôle lui-même. Voir l'explication de Ralph Pini au sujet de la décision de sa compagnie, en 2016, de cesser la fabrication de matériel. Brian Heater, « [BlackBerry's device head outlines the company's post-hardware future](#) », *TechCrunch*, 29 septembre 2016.
31. Benedict Evans, analyste pour la société de capital de risque Andreessen Horowitz, dont le siège est dans la Silicon Valley, prévoit qu'il y aura bientôt cinq milliards d'utilisateurs de téléphones intelligents dans le monde. Il signale qu'en juin 2016, l'utilisation des applications pour téléphones intelligents représentait 60 % du temps passé en ligne aux États-Unis. Voir Benedict Evans, « [Mobile is eating the world](#) » (diaporama PowerPoint), Andreessen Horowitz, décembre 2016.
32. Par exemple, les applications interagissent avec le système d'exploitation sous-jacent des appareils mobiles. Elles peuvent aussi interagir avec des services dorsaux (back-end services), comme quand une application bancaire mobile permet à un utilisateur de transférer des fonds à un tiers. Des individus malveillants peuvent aussi utiliser des applications contrefaites pour bernier des consommateurs en les incitant à fournir leurs identifiants et d'autres renseignements personnels de nature délicate durant le processus de téléchargement des applications en cause.
33. Les risques que posent pour la sécurité les applications gratuites et de source ouverte sont bien connus, mais les applications conçues à l'interne par les fournisseurs de TIC eux-mêmes présentent aussi des problèmes. Une étude récente de l'Institut Ponemon portant sur 640 entreprises a révélé qu'en moyenne seulement 29 % des applications mobiles font l'objet de tests de vulnérabilité et 33 % ne subissent absolument aucun test; 69 % des répondants au sondage de Ponemon ont expliqué la vulnérabilité des codes de certaines applications par les pressions subies pour mettre les applications en marché le plus rapidement possible. Ponemon Institute, [2017 Study on Mobile & IoT Application Security](#), étude menée de manière indépendante pour le compte d'IBM et Arxan Technologies, janvier 2017 (inscription gratuite requise).
34. Voir, par exemple, Tom Spring, « [Bad Code Library Triggers Devil's Ivy Vulnerability in Millions of IoT Devices](#) », *Threat Post* (blogue), 19 juillet 2017.

35. Les puces – qu'on appelle aussi parfois « microplaquettes semi-conductrices », parce que le matériau dans lequel elles sont fabriquées, le silicium, est un semi-conducteur – sont le cerveau des appareils numériques. Par le jeu d'interrupteurs, les circuits intégrés des puces traduisent le code binaire en commande. Les programmeurs travaillent normalement dans des programmes en langage naturel, comme Perl ou C++, mais, au niveau matériel, ces entrées sont lues au moyen d'un système binaire reposant sur les valeurs 1 et 0. Habituellement, des programmes intermédiaires qu'on appelle « compilateurs » convertissent le langage de programmation en langage machine. Pour voir du texte en langage naturel converti en code binaire, consulter [Convert text to binary](http://unit-conversion.info), unit-conversion.info.
36. Clair Brown et Greg Linden, [Semiconductor Capabilities in the U.S. and Industrializing Asia](#), document présenté à l'occasion de la Conférence annuelle de 2008 des Industry Studies Alfred P. Sloan, Boston, 1<sup>er</sup> et 2 mai 2008, p. 4.
37. Voir IC Insights, [Taiwan Maintains Largest Share of Global IC Wafer Fab Capacity](#), communiqué, 23 février 2017.
38. Lorsque les observateurs américains en matière de sécurité parlent de « délocalisation » ou de « relocalisation » des TI, ils font généralement référence au rapatriement de toutes les étapes de la production sur un territoire contrôlé par les États-Unis.
39. Le *New York Times* a fait état de notes de service de la National Security Agency (NSA) ayant fait l'objet de fuites selon lesquelles l'Agence avait pris le contrôle d'un processus d'élaboration de normes de cryptographie à base de courbes elliptiques dirigé par le Centre de la sécurité des télécommunications (CST). Selon l'article du *New York Times*, l'une des notes de service précise qu'après quelques tractations en coulisses avec le chef de la délégation canadienne et avec le CST, la table était mise pour que la NSA propose une nouvelle version de l'ébauche. Selon des observateurs, cela laisse entrevoir la possibilité que le CST était au courant des intentions de la NSA et qu'il l'a laissée faire. Voir Nicole Perlroth, « [Government Announces Steps to Restore Confidence on Encryption Standards](#) », *New York Times*, 10 septembre 2013. Voir aussi la note suivante.
40. La technologie de chiffrement en cause fait référence à un algorithme dans un générateur de bits pseudo-aléatoire appelé Dual\_EC\_DRBG. Il est nécessaire de pouvoir compter sur de bonnes sources de nombres aléatoires pour générer des clés de chiffrement ne pouvant être décryptées et, pour diverses raisons, il a été démontré que l'algorithme Dual\_EC\_DRBG peut générer des résultats prévisibles. On dit que la NSA a versé à RSA, un important fabricant de produits de chiffrement, 10 millions de dollars pour faire du Dual\_EC\_DRBG la source d'entropie par défaut de ses produits de chiffrement, permettant ainsi à l'Agence de disposer d'une porte dérobée lui donnant accès à tout ce qui est chiffré au moyen de clés produites à partir de cette source. Voir Nick Sullivan, « [How the NSA \(may have\) put a backdoor in RSA's cryptography: A technical primer](#) », *Ars Technica*, 5 janvier 2014.  
  
Des articles fondés sur des documents divulgués par Edward Snowden indiquent que le CST soit a été favorable soit ne s'est pas réellement opposé à ce que la NSA pousse pour que le Dual\_EC\_DRBG devienne une norme internationale. Voir, par exemple, Jesse Brown, « [NSA says it 'finessed' Canada, seizing control of global crypto](#) », *Macleans*, 11 septembre 2013; Kim Zetter, « [New Discovery Around Juniper Backdoor Raises More Questions about the Company](#) », *Wired*, 8 janvier 2016; et Omar El Akkad, « [The strange connection between the NSA and an Ontario tech firm](#) », *Globe and Mail*, 20 janvier 2014.
41. Gus W. Weiss, « [The Farewell Dossier: Duping the Soviets](#) », *Studies in Intelligence*, Central Intelligence Agency Center for the Study of Intelligence (États-Unis), 14 avril 2007.



42. Voir Radio-Canada, *Bon baiser du Canada (From Canada with Love)*, 10 janvier 2013. Pour visionner un extrait de ce documentaire dans lequel le président de la compagnie est interviewé au sujet de l'opération, voir Vincent Frigon, « [Bon baiser du Canada – From Canada with Love – Extrait 4](#) », *YouTube*, publié le 10 janvier 2013.
43. Il convient de noter qu'en ce qui concerne la fabrication de logiciels et de matériel informatique, le présent document confère une portée étroite à l'expression « sécurité de la cyberchaîne d'approvisionnement ». Cette expression est aussi souvent utilisée pour décrire le problème plus vaste des risques que présentent les fournisseurs de services de TI pour la sécurité des organisations. Les récentes et graves atteintes à la sécurité des renseignements des cartes de crédit de clients de Home Depot et de Target sont un exemple de ce problème dans la chaîne d'approvisionnement, en ce sens que ces attaques ont commencé par le piratage de fournisseurs tiers. Pour en savoir plus sur ces incidents, voir Brian Krebs, « [Home Depot: Hackers Stole 53M Email Addresses](#) », *Krebs on Security* (blogue), 7 novembre 2014. Pour en apprendre davantage sur la sécurité de la chaîne d'approvisionnement des logiciels, voir Carol Woody et Robert J. Ellison, *Supply-Chain Risk Management: Incorporating Security into Software Development*, Software Engineering Institute, Université Carnegie Mellon, mars 2010.
44. Cela dit, on a récemment appris que même le département américain de la Défense utilise des antivirus provenant d'un fournisseur russe, Kaspersky, ce qui laisse supposer que l'interdiction complète est difficile à faire respecter. Voir Nicholas Weaver, « [On Kaspersky](#) », *Lawfare* (blogue), 25 juillet 2017; et Saqib Shah, « [FBI reportedly advising companies to ditch Kaspersky apps](#) », *Engadget*, 21 août 2017.
45. Insikt Group, « [China's Cybersecurity Law Gives the Ministry of State Security Unprecedented New Powers Over Foreign Technology](#) », *Recorded Future* (blogue), 31 août 2017.
46. « [Putin tells Russia's tech sector: Ditch foreign software or lose out](#) », *CNBC*, 9 septembre 2017.
47. Dustin Volz, Joel Schectman et Jack Stubbs, « [Tech firms let Russia probe software widely used by U.S. government](#) », *Reuters*, 25 janvier 2018.
48. Joel Schectman, Dustin Volz et Jack Stubbs, « [Under pressure, Western tech firms bow to Russian demands to share cyber secrets](#) », *Reuters*, 23 juin 2017.
49. Voir Royaume-Uni, Cabinet Office, National Security Secretariat, *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2017: A report to the National Security Adviser of the United Kingdom*, avril 2017. Voir aussi Electronic Warfare Associates-Canada, Ltd. (EWA-Canada), *High Assurance Testing*; Nestor Arellano, « [Ontario, Huawei Canada partner in \\$300M 5G project](#) », *Canadian Government Executive*, 9 mars 2016; et Rose Behar, « [What Huawei's historic 5G test means for the future of wireless in Canada](#) », *mobilesyrup*, 17 juillet 2017.
50. Pour une étude sur l'espérance de vie moyenne des vulnérabilités du jour zéro et de la façon dont elles sont utilisées, voir Lillian Ablon et Timothy Bogart, *Zero Days. Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, RAND Corporation, 2017.
51. Voir Ben Buchanan, *Nobody But Us: The Rise and Fall of the Golden Age of Signals Intelligence*, Aegis Series Paper n° 1708, Hoover Institution, Université Stanford, 30 août 2017.

52. Le « Groupe des cinq » fait référence à l'alliance conclue pendant la Seconde Guerre mondiale entre les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande pour la collecte de renseignements électromagnétiques. Cette alliance existe toujours et sert de fondement à la coopération entre les organismes de sécurité nationale et d'application de la loi de ces cinq pays. Il convient aussi de noter que le Centre de la sécurité des télécommunications (CST) collabore et échange des renseignements avec des entités étrangères autres que le Groupe des cinq.
53. Le respecté expert américain de la cryptographie Bruce Schneier soutient depuis longtemps que l'approche du « personne d'autre que nous » n'est pas un concept utile et que les activités de cyberdéfense de la NSA sont trop souvent négligées par rapport aux activités de cyberoffensive. Voir, par exemple, Bruce Schneier, « [Simultaneous Discovery of Vulnerabilities](#) », *Schneier on Security* (blogue), 25 février 2016.
54. Pour lire un résumé de l'opinion récente d'un expert sur la question, voir Taylor Armerding, « [Should governments keep vulnerabilities secret?](#) », *Naked Security*, 1<sup>er</sup> août 2017. Voir aussi Bruce Schneier, « [WannaCry and Vulnerabilities](#) », *Schneier on Security* (blogue), 2 juin 2017; et Benjamin Dean, « ['Zero-day' stockpiling puts us all at risk](#) », *The Conversation* (blogue), 4 août 2015.
55. Rick Ledgett, « [No, the U.S. Government Should Not Disclose All Vulnerabilities in Its Possession](#) », *Lawfare* (blogue), 7 août 2017.
56. *Ibid.*
57. Voir Bruce Schneier, « [Heartbleed](#) », *Schneier on Security* (blogue), 9 avril 2014; et Valerie Boyer, « [CSEC aware of Heartbleed bug day before CRA website shutdown](#) », *CBC News*, 16 avril 2014.
58. Michael Daniel, « [Heartbleed: Understanding When We Disclose Cyber Vulnerabilities](#) », *The White House* (blogue), 28 avril 2014.
59. Voir, par exemple, Matthew Braga, « [When do Canadian spies disclose the software flaws they find? There's a policy, but few details](#) », *CBC News*, 6 septembre 2017.
60. Le projet de loi intitulé Protecting our Ability To Counter Hacking (PATCH) Act of 2017 est parrainé par les sénateurs Brian Schatz (D-Hawaï), Ron Johnson (R-Wisconsin) et Cory Gardner (R-Colorado) et les représentants Ted Lieu (D-Californie) et Blake Farenthold (R-Texas). Voir Congrès des États-Unis [S.1157 – PATCH Act of 2017](#) et [H.R.2481 – PATCH Act of 2017](#). Pour un aperçu du projet de loi proposé, voir Mailyn Fidler et Trey Herr, « [PATCH: Debating Codification of the VEP](#) », *Lawfare* (blogue), 17 mai 2017.
61. Le chiffrement de bout en bout fait en sorte que seuls l'expéditeur et le destinataire d'une communication chiffrée peuvent la lire, car cette communication est chiffrée directement à partir de leur appareil au moyen d'une clé qu'ils sont les seuls à posséder. Pour en savoir plus, voir Andy Greenberg, « [Hacker Lexicon: What is end-to-end encryption?](#) », *Wired*, 25 novembre 2014.
62. Zack Whittaker, [Meet 'Muscular': NSA accused of tapping links between Yahoo, Google datacenters](#), *ZDNet*, 30 octobre 2013.
63. Danny Yadron, « [Facebook, Google and WhatsApp plan to increase encryption of user data](#) », *The Guardian*, 14 mars 2016.
64. Megan Squire, « [End-to-end encryption isn't enough security for 'real people'](#) », *The Conversation* (blogue), 13 août 2017. Voir aussi Jim Bronskill, « [Five Eyes alliance stress 'more timely and detailed' information sharing to detect terrorists](#) », *Toronto Star*, 28 juin 2017. Voir aussi, Sécurité publique Canada, [Réunion ministérielle des cinq pays 2017 : Communiqué conjoint](#), 27 juin 2017.
65. Robert Cribb, Dave Seglins et Chelsea Gomez, « [Top Mountie lobbying PM for greater digital surveillance powers](#) », *Toronto Star*, 16 novembre 2016.



66. *Ibid.*
67. Michael Hayden a aussi été directeur de la Central Intelligence Agency (CIA) des États-Unis de 2006 à 2009, mais il préconise des mesures de chiffrement rigoureuses d'après son expérience à titre de directeur de la NSA.
68. Pour en savoir plus sur les méthodes permettant d'avoir accès à du contenu en texte clair grâce aux vulnérabilités aux points terminaux, voir Orin S. Kerr et Bruce Schneier, « [Encryption Workarounds](#) », ébauche du 20 mars 2017, *Georgetown Law Journal* [À PARAÎTRE], Faculté de droit de l'Université George Washington, document de recherche en droit public n° 2017-22, Université George Washington, document de recherche en études juridiques n° 2017-22.
69. Voir Tom DiChristopher, « [US safer with fully encrypted phones: Former NSA/CIA chief](#) », *CNBC*, 23 février 2016; et « [End-to-end encryption back door 'a bad idea'](#) », *BBC News*, 10 juillet 2017.
70. Steve Morgan, « [Cybercrime damages expected to cost the world \\$6 trillion by 2021](#) », *CSO*, 22 août 2016.
71. Voir Corporation for National Research Initiatives, [Overview of the Digital Object Architecture](#), 28 juillet 2012; et Sally Adee et Carl Miller, « [We can stop hacking and trolls, but it would ruin the internet](#) », *New Scientist*, 9 août 2017.
72. Vinton Cerf est souvent et à tort le seul à recevoir le crédit pour l'invention du protocole TCP/IP.
73. Dans l'architecture TCP/IP actuelle, les utilisateurs ont besoin d'une adresse IP pour trouver un serveur branché à Internet en particulier et d'une adresse Uniform Resource Locator (URL) pour trouver le répertoire précis sur ce serveur où la ressource documentaire qu'ils cherchent se trouve. Quiconque a déjà ajouté un article en ligne dans ses favoris pour se rendre compte que le lien ne fonctionne plus une semaine plus tard connaît les lacunes de ce système. Dans la mesure où l'on garde les métadonnées à jour, l'attribution d'un *handle* à une ressource documentaire résout le problème du lien mort et veille à ce que la ressource documentaire demeure accessible à ceux qui ont droit d'y avoir accès.
74. Selena Larson, « [A smart fish tank left a casino vulnerable to hackers](#) », *CNNTech*, 19 juillet 2017.
75. Voir, par exemple, Freedom House, [Freedom in the World 2018: Democracy in Crisis](#).
76. Voir, par exemple, Robert Coalson, « [New Kremlin Information-Security Doctrine Calls For 'Managing' Internet In Russia](#) », *Radio Free Europe/Radio Liberty*, 6 décembre 2016. Voir aussi Timothy Thomas, « Information Security Thinking: A Comparison of U.S., Russian, And Chinese Concepts », *The Science and Culture Series, Nuclear Strategy and Peace Technology, International Seminar on Nuclear War and Planetary Emergencies*, juillet 2001, p. 344 à 358.
77. L'Union internationale des télécommunications (UIT) est l'organisme des Nations Unies spécialisé dans les technologies de l'information et des communications.
78. « [What Governments Decided on Digital Object Architecture for IoT](#) », *Wiley Connect* (blogue), 8 novembre 2016. Le billet dit également que la norme prédominante de l'Union internationale des télécommunications relativement à la découverte des informations relatives à la gestion de l'identité se fonde déjà sur l'architecture d'objet numérique, même si elle ne fait pas mention des *handles* ou du système Handle. Voir aussi Union internationale des télécommunications, [X.1255 : Cadre pour la découverte des informations relatives à la gestion d'identité](#), 4 septembre 2013.

- Il convient aussi de noter qu'un grand nombre de personnes considèrent l'AON comme étant une technologie relativement âgée et imparfaite. Par exemple, la Commission d'études 20 de l'UIT mène actuellement un examen sur la contrefaçon dans l'AON. Ses travaux semblent avoir servi de fondement à une résolution présentée à l'Assemblée mondiale de normalisation des télécommunications de l'UIT organisée en Tunisie en 2016. Voir Secteur de la normalisation des télécommunications de l'UIT (UIT-T), [Résolution 96 – Études du Secteur de la normalisation des télécommunications de l'UIT visant à lutter contre la contrefaçon des dispositifs de télécommunication/technologies de l'information et de la communication](#), Hammamet, Tunisie, 25 octobre au 3 novembre 2016.
79. Un domaine de premier niveau correspond au dernier segment d'un nom de domaine ou à ce qui suit le point, comme.com ou.org.
  80. Société pour l'attribution des noms de domaine et des numéros sur Internet, [About ICANN](#).
  81. Par exemple, la version 6 de l'IP (IPv6), la prochaine version du protocole servant à représenter l'espace d'adressage dans Internet, pourrait être mise en œuvre de manière à ce qu'on puisse attribuer des adresses IP fixes à chaque appareil branché sur la planète. Toutefois, des adresses IPv6 peuvent aussi être attribuées de manière dynamique et aléatoire au moyen d'extensions qui protègent l'identité des utilisateurs.
  82. Pour en savoir plus, voir Bureau des affaires de désarmement des Nations Unies, [Les progrès de l'informatique et de la télématique et la question de la sécurité internationale](#). Voir aussi Geneva Internet Platform (Digital Watch Observatory en partenariat avec l'Internet Society), [UN GGE](#).
  83. Assemblée générale des Nations Unies, [Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale](#), 70<sup>e</sup> session, Point 93 de l'ordre du jour provisoire, n° A/70/174, 22 juillet 2015.
  84. Même s'ils sont d'avis que le Groupe d'experts gouvernementaux des Nations Unies doit demeurer la tribune de discussion des cybernormes, Melissa Hathaway, Joseph S. Nye et Eneken Tikk soulèvent tous, dans un rapport récent, des questions quant aux progrès accomplis jusqu'à maintenant. Voir Fen Osler Hampson et Michael Sulmeyer (dir.), [Getting beyond Norms: New Approaches to International Cyber Security Challenges](#), Centre for International Governance Innovation, 7 septembre 2017.
  85. Voir Assemblée générale des Nations Unies, [Lettre datée du 9 janvier 2015, adressée au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie, du Kazakhstan, du Kirghizistan, de l'Ouzbékistan et du Tadjikistan auprès de l'Organisation des Nations Unies](#), 69<sup>e</sup> session, Point 91 de l'ordre du jour, n° A/69/723, 13 janvier 2015.
  86. Nations Unies, [La Charte des Nations Unies](#).
  87. Voir Assemblée générale des Nations Unies, [Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale](#), 68<sup>e</sup> session, Point 94 de l'ordre du jour provisoire, n° A/68/98, 24 juin 2013 (publié de nouveau pour des raisons techniques le 30 juillet 2013).
  88. Julian Ku, [How China's Views on the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare](#), Aegis Series Paper n° 1707, Hoover Institution, Université Stanford, 17 août 2017.

89. L'affaire du *Caroline* renvoie à un événement historique qui a donné lieu à la doctrine de la légitime défense préventive. En 1837, une crise diplomatique survient lorsqu'un navire américain qui vient prêter main-forte à des rebelles canadiens se réfugie dans l'île Navy, sur la rivière Niagara, avec l'aide d'Américains des environs. Franchissant la frontière internationale, les forces britanniques montent à bord du *Caroline*, tuent un membre américain de l'équipage, puis entraînent le navire dans le courant, y mettent le feu et le font dériver vers les chutes Niagara. Les Britanniques prétendent plus tard qu'ils ont attaqué le *Caroline* en légitime défense. Le secrétaire d'État américain de l'époque soutient pour sa part que l'argument de la légitime défense n'est justifié que si l'intervention est proportionnelle à la menace et si cette dernière est pressante, écrasante, ne permet pas le choix des moyens et ne laisse pas de temps pour délibérer. C'est ce qu'on a appelé plus tard le « critère du *Caroline* ». Voir Christine D. Grey, *International Law and the Use of Force*, 3<sup>e</sup> éd., Oxford University Press, 2008; et Ryan J. Hayward, « [Evaluating the "Imminence" of a Cyber Attack for Purposes of Anticipatory Self-Defense](#) », *Columbia Law Review*, vol. 117, n<sup>o</sup> 2.
90. Julian Ku (2017), p. 14 [TRADUCTION].
91. En effet, selon les termes mêmes employés par le Centre de la sécurité des télécommunications, « le renseignement électromagnétique étranger du CST a joué un rôle vital dans [la formulation] des avertissements en temps opportun pour contrer les cybermenaces à l'endroit du gouvernement du Canada ainsi que des réseaux et de l'infrastructure d'information essentielle ». (Centre de la sécurité des télécommunications, [Renseignement électromagnétique](#).) Le projet de loi C-59, Loi concernant des questions de sécurité nationale, propose l'établissement d'un nouveau mandat pour le CST, qui lui permettrait de mener des « cyberopérations actives » en vue de « réduire, d'interrompre, d'influencer ou de contrecarrer, selon le cas, les capacités, les intentions ou les activités de tout étranger ou État, organisme ou groupe terroriste étrangers, dans la mesure où ces capacités, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité, ou afin d'intervenir dans le déroulement de telles intentions ou activités ». Cela semble préparer la voie à la tenue d'activités de légitime défense préventive par le CST. Voir [Projet de loi C-59 : Loi concernant des questions de sécurité nationale](#), 1<sup>re</sup> session, 42<sup>e</sup> législature, art. 20 de la Loi constituant le Centre de la sécurité des télécommunications figurant à l'art. 76 du projet de loi (première lecture, 20 juin 2017).
92. Le professeur Zhixiong Huang, de l'Institut de droit international de l'Université Wuhan, est membre du Groupe d'experts internationaux ayant contribué au texte.
93. Julian Ku, « [Tentative Observations on China's Views on International Law and Cyber Warfare](#) », *Lawfare* (blogue), 26 août 2017.
94. « Rule 73 – Imminence and immediacy », dans *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2<sup>e</sup> éd., Michael N. Schmitt (dir.), préparé par le groupe d'experts international à la demande du Centre d'excellence de cyberdéfense coopérative de l'OTAN, Cambridge University Press, 2017, p. 351.

95. La protection de la propriété intellectuelle est évidemment une autre préoccupation importante. Il existe certes un régime juridique international pour la protection du droit d'auteur, mais ce ne sont pas tous les États qui sont parties à toutes les conventions ni tous les membres adhérant aux conventions qui respectent leurs obligations de manière égale. Par exemple, la Chine adhère à l'[Accord sur les ADPIC \[aspects des droits de propriété intellectuelle qui touchent au commerce\]](#) de l'Organisation mondiale du commerce et au [Traité de l'OMPI sur le droit d'auteur \[Organisation mondiale de la propriété intellectuelle\]](#), qui traitent tous deux du code logiciel. Or, les entreprises chinoises se font souvent accuser de violer le droit d'auteur, et le vol de propriété intellectuelle est un aspect clé des activités d'espionnage de la Chine depuis la fin des années 1970. Parallèlement, dans sa stratégie nationale de 2008 sur la propriété intellectuelle, la Chine laisse entendre qu'elle compte être en mesure de générer, d'utiliser et de protéger la propriété intellectuelle d'ici 2020. Voir V.K. Unni, « [Specialized Intellectual Property Enforcement in China: Implications for Indian Companies](#) », *LiveLaw.in* (blogue), 6 septembre 2017; et Royaume-Uni, Intellectual Property Office, [Software Copyright Registration in China, know before you go](#), retransmis par le Berkman Klein Center for Internet and Society de l'Université Harvard, 2013.