Il est non viable, et même dangereux, d'envisager de rafistoler notre avenir numérique

Melissa Hathaway

Les technologies novatrices du vingtième siècle ont profondément transformé la société et l'économie. Le premier message électronique a été envoyé il y a près de 50 ans, le 29 octobre 1969 (sur l'Advanced Research Projects Agency Network, ou ARPANET, le réseau qui a servi de base à l'Internet), mais ce n'est que lors de l'introduction du domaine de premier niveau .com, en 1985, que l'Internet est devenu un moteur de commerce (Hathaway, 2012). Le commerce électronique a été facilité par le lancement du World Wide Web, en 1990, puis a été accéléré, d'une part, par la puissance informatique abordable intégrée et assortie de fonctions et, d'autre part, par un vaste éventail d'applications à portée de main (téléphones mobiles). Depuis, tant les nations que les entreprises ont accueilli à bras ouverts et adoptés les technologies de l'information et des communications (TIC), les ont intégrées à leurs réseaux et à leurs infrastructures et ont bénéficié d'une croissance économique et commerciale exponentielle grâce à l'amélioration de leurs services, à une productivité accrue et à une diminution de leurs coûts. Aujourd'hui, l'économie numérique représente environ 20 % du PIB mondial (Wladawsky-Berger, 2017; Huawei and Oxford Economics, 2017) et, d'ici à 2020, au moins 20 milliards d'appareils d'Internet des objets (IoT) hyper-connecteront les infrastructures et les entreprises de nos pays pour générer un revenu mondial de 8 trilliards de dollars (Cleo, 2018).

Il n'en reste pas moins que cette transformation numérique, qui repose sur des communications abordables et des appareils bon marché, s'accompagne de nouveaux risques, qui ne peuvent pas être ignorés. La décision d'accueillir à bras ouverts et d'intégrer des technologies commerciales bon marché souvent mal codées ou mal conçues dans chaque volet de notre société connectée, des systèmes gouvernementaux aux ménages, en passant par les infrastructures essentielles, les services et les entreprises, n'est pas sans conséquences. Les fournisseurs de ces technologies, les vendeurs de TIC, sont encouragés à être les premiers à commercialiser leurs produits, et le marché a simplement accepté leur promesse de réparer ou de « rafistoler » les défauts de leurs produits plus tard. Par exemple, Microsoft a officialisé ce processus de rafistolage régulier, maintenant connu sous le nom de « patch Tuesday » (mardi du rafistolage), en octobre 2003. D'autres fournisseurs procèdent à ce type de rattrapage moins régulièrement, et sans faire preuve de transparence concernant les vulnérabilités connues qu'ils ont transmises à nos produits et à nos services numériques. Le *patch Tuesday* est inévitablement suivi d'un « vulnerable Wednesday » (mercredi vulnérable) au cours duquel des acteurs malveillants, qui sont maintenant aussi au courant de ces nouvelles vulnérabilités révélées, peuvent exploiter des systèmes non rafistolés pour voler des données sensibles, nuire à des entreprises hors ligne et, dans certains cas, détruire des systèmes de TI qui alimentent des entreprises et des services essentiels. De plus, la majorité des organisations ne sont pas en mesure de mettre à jour promptement leurs systèmes lorsque des correctifs sont émis, ce qui accroît d'autant plus notre vulnérabilité collective aux méfaits cybernétiques.

La norme de référence pour la mise en place d'un correctif logiciel est 30 jours (Proviti, 2017). Certaines organisations peuvent avoir besoin de plus de temps pour faire une mise à jour logicielle afin de tester correctement leurs systèmes en vue de veiller à ce que d'autres applications ou processus ne soient pas touchés. D'autres organisations peuvent, cependant, choisir de ne pas mettre à jour leurs logiciels par crainte de briser de vieilles applications au sein de systèmes plus anciens arrivant très probablement en fin de vie. Pour mettre cette théorie en perspective, le *patch Tuesday* effectué par Microsoft en avril 2019 comprenait 15 correctifs logiciels visant à remédier à au moins 74 vulnérabilités de ses systèmes d'exploitation et de ses logiciels de soutien Windows, dont deux bogues Zero Day (Krebs, 2019a). De même, la mise à jour corrective précédente de mars 2019 portait sur plus de 60 vulnérabilités des systèmes d'exploitation de Windows, d'Internet Explorer, d'Edge, d'Office et de Sharepoint (Krebs, 2019b). Cette philosophie de la « mise en marché maintenant, correction ensuite » a accru notre exposition aux bogues et entraîné de véritables pertes économiques. Par exemple, le cybercrime croît à une vitesse de 26 % par année, et on estime qu'il en coûtera au moins 2,1 trilliards de dollars US à l'économie mondiale en 2019, ou 2 % du PIB mondial (Symantec, 2018). De plus, les attaques IoT ont augmenté de 600 % entre 2016 et 2017, en grande partie à cause de la facilité d'exploitation des appareils connectés (ibid.).

Or, la facilité déconcertante avec laquelle il est possible d'exploiter ces vulnérabilités est souvent méconnue du grand public et des décideurs. Par exemple, Shodan, un moteur de recherche gratuit et accessible au public conçu pour localiser

Melissa Hathaway s'est jointe au Conseil d'administration du CIGI en mars 2019. Elle est la présidente de Hathaway Global Strategies LLC, où elle enrichit la consultation stratégique et la formulation de stratégies d'une perspective pluridisciplinaire et multi-institutionnelle pour des clients des secteurs public et privé. Elle a œuvré au sein de deux administrations présidentielles américaines : elle a dirigé l'initiative nationale globale de la cybersécurité sous le mandat du président George W. Bush et piloté l'examen de la politique sur le cyberespace pour le président Barack Obama.

Au Royaume-Uni, WannaCry a affecté au moins 81 des 236 fiducies du service national de santé en mettant de l'équipement médical hors d'usage, ce qui a grandement nui à la santé et à la sécurité publiques (National Audit Office, 2017). (Photo : Pegasus Pics / Shutterstock.com)

des appareils connectés peut servir à trouver aisément des systèmes défectueux (Hill, 2013). Les outils utilisés pour exploiter des vulnérabilités connues sont également peu dispendieux et faciles à manier. Que vous achetiez l'ouvrage intitulé *Hacking for Dummies* (le piratage pour les débutants), ou engagiez un professionnel du Web invisible, la capacité de faire du mal n'est plus l'apanage des États-nations. Une attaque de déni de service distribué peut être exécutée pour seulement 700 $ US, tandis que les crédits bancaires volés peuvent être acquis au prix d'un petit pain (Barysevich, 2017). L'accès non autorisé à des comptes sur Instagram, Twitter, Snapchat ou d'autres plateformes de médias sociaux coûte juste un peu plus de 100 $ US (McCamy, 2018; Dell SecureWorks, 2016). Si vous souhaitez faire du tort à une entreprise, il ne vous en coûtera peut-être que 500 $ US pour pirater sa boîte de courriel. En 2017, les problèmes causés aux courriels des entreprises ont occasionné des pertes de plus de 650 millions de dollars US aux États-Unis seulement (Federal Bureau of Investigation, 2017).

Le coût de la cyberinsécurité mondiale

Les conséquences économiques et sociétales de cette vulnérabilité répandue deviennent de plus en plus aiguës. Le monde est témoin d'un nombre croissant d'incidents cybernétiques très médiatisés qui menacent la santé et la sécurité publiques, le transport et le commerce mondiaux ainsi que des fabricants industriels clés. Par exemple, en mai 2017, une souche particulièrement simple de rançongiciels connue sous le nom de WannaCry a ciblé des lacunes des systèmes d'exploitation de Microsoft Windows, ce qui a porté atteinte à des millions d'ordinateurs, dans 150 pays et dans tous les secteurs. Cette attaque mondiale a paralysé des activités de fabrication ainsi que des systèmes de transport et de télécommunications. Selon le National Audit Office du Royaume-Uni, WannaCry a affecté au moins 81 des 236 fiducies du service national de santé en mettant de l'équipement médical hors d'usage, ce qui a grandement nui à la santé et à la sécurité publiques (National Audit Office, 2017).

Six semaines plus tard, en juin 2017, un logiciel destructeur malveillant, connu sous le nom de NotPetya, a balayé le monde, réduisant en quelques minutes le capital social de centaines d'entreprises à néant. Les activités commerciales de nombreuses entreprises, dont Maersk (expédition), Merck (produits pharmaceutiques), Mondelez (confections) et DLA-Piper (services juridiques) ont immédiatement cessé. Shipping giant A.P. Moller-Maersk a été l'une des entreprises les plus touchées par cette attaque. Elle est responsable de la gestion de 76 installations portuaires du monde entier et d'environ 20 % de la capacité d'expédition par conteneurs du monde (Reuters, 2017). Au propre comme au figuré, elle était finie après que NotPetya ait eu contaminé l'ensemble de son réseau mondial. En quelques minutes, le virus a chiffré et éradiqué les systèmes mondiaux de technologie de l'information de l'entreprise, soit, entre autres, 4 000 serveurs, 45 000 ordinateurs et 2 500 applications de 600 installations réparties entre 130 pays. Les systèmes de Maersk ont été hors ligne pendant plus de 150 heures (le revenu horaire de Maersk s'élève, en moyenne, à 2,9 millions de dollars US); cette entreprise a subi une perte de l'ordre de 435 millions de dollars US pour remplacer les systèmes de TI qui alimentaient ses affaires (A.P. Moller-Maersk, 2017). En fin de compte, elle a perdu 10 % de sa part de marché au profit de la China Ocean Shipping Company. Pour les actionnaires, la valeur de Maersk s'est dépréciée de 30 % au cours des neuf mois suivant l'incident et de plus de 50 % 18 mois après l'incident[1]. Le PIB du Danemark a aussi subi des répercussions du fait que Maersk contribuait à hauteur d'au moins 7 % au PIB du pays. Les conséquences de deuxième et troisième ordre pour les expéditions et l'économie mondiales n'ont pas été quantifiées (Greenberg, 2018).

Aujourd'hui, les cadres supérieurs de Maersk soulignent l'importance des activités de rétablissement en raison des efforts incommensurables que leur entreprise a dû déployer pour reprendre ses activités commerciales en ligne (Palmer, 2019). Cependant, Maersk était conscientes de ses vulnérabilités numériques et de la nécessité d'effectuer des améliorations sur le plan de la cybersécurité avant même l'apparition de NotPetya (A.P. Moller-Maersk, 2016). Elle aurait mieux survécu à cette tempête si elle avait mis en œuvre des procédures de sécurité standards, telles que des mises à jour régulières de ses logiciels et de ses systèmes d'exploitation ainsi qu'une segmentation de son réseau.

Les problèmes économiques causés par NotPetya et WannaCry se chiffrent par centaines de milliards de dollars. On craint toutefois que des entreprises d'envergure mondiale ne soient toujours pas préparées à faire face à la flambée mondiale d'un autre rançongiciel ou d'une autre attaque destructive. Durant le premier trimestre de 2019, le nouveau rançongiciel LockerGoga a exploité des systèmes de Microsoft non corrigés pour mettre hors ligne la firme d'ingénierie-conseil française Altran Technologies, le fabricant de produits optiques japonais HOYA Corporation, les entreprises chimiques américaines Hexion et Momentive (Franceschi-Bicchierai, 2019) ainsi que Norwegian Norsk Hydro, l'un des plus grands fabricants d'aluminium du monde (Ashford, 2019).

Les outils utilisés pour exploiter des vulnérabilités connues sont également peu dispendieux et faciles à manier.

Plus les entreprises relient et assujettissent leurs activités commerciales à l'IoT, plus elles exposent leurs produits à des vulnérabilités, dont l'exploitation augmentera aussi, ce qui met leurs activités d'affaires en danger. C'est pourquoi il faut remédier aux vulnérabilités logicielles et matérielles lors des phases de développement et de conception qui précèdent les activités industrielles actives qui revêtent des enjeux importants. Les infrastructures essentielles, telles que les réseaux énergétiques, les centres de fabrication et les usines pétrochimiques, subissent de plus en plus d'attaques de logiciels malveillants conçus pour infiltrer des systèmes de contrôles industriels (SCI) en vue de désactiver et de perturber le matériel informatiques ou d'en prendre le contrôle. Par exemple, le logiciel malveillant Triton a été conçu pour saboter la technologie d'exploitation critique des SCI, cartographier le réseau industriel et permettre aux attaquants de contrôler les systèmes à distance (Sobczak, 2019). Le premier exemple de son utilisation a été découvert en 2017 dans une installation pétrochimique du Moyen-Orient. Bien que, dans sa conception, Triton comportait de lacunes, il aurait pu servir à contrecarrer les procédures d'arrêt qui empêchent normalement

Quelles que soient leur ampleur et leur portée, les stratégies nationales de cybersécurité échoueront en l'absence d'une hiérarchie des responsabilités claire qui détermine les obligations de sécurité qui incombent à chaque partie.

des catastrophes, tels que des explosions ou la fuite de produits chimiques toxiques (Giles, 2019; Vijayan, 2017; Jackson, Higgins 2018). Ce logiciel malveillant a tiré parti d'une vulnérabilité du système de sécurité instrumenté Triconex de Schneider Electric. Ce système est déployé dans d'innombrables secteurs répartis entre 73 pays, notamment dans les domaines du raffinage, de la production d'électricité et des produits pétrochimiques, chimiques, chimiques spécialisés et pharmaceutiques (Desruisseaux, 2018). Au fur et à mesure que les fabricants industriels amorcent leur transformation numérique pour automatiser leurs processus et intégrer l'IoT à leurs gammes de produits et de services, leur risque de subir une perturbation numérique et la destruction de leurs actifs augmente aussi. L'utilisation de logiciels malveillants sophistiqués pour cibler ces systèmes ne cesse d'augmenter, et est alarmante.

Comportement interétatique dans l'espace cybernétique : l'hostilité à la hausse

Le danger d'une cyberhostilité interétatique est également imminent. Selon la National Intelligence Strategy des États-Unis de 2019, les cybermenaces poseront un risque accru en matière de santé publique, de sécurité et de prospérité, à mesure que les technologies de l'information s'intégreront aux infrastructures essentielles, aux réseaux nationaux névralgiques et aux périphériques des consommateurs (Office of the Director of National Intelligence, 2019). La cyberinsécurité nuit à notre économie et déstabilise notre sécurité. Chaque vulnérabilité est à un clic de se faire exploiter à l'aide d'armes et de services abordables et facilement accessibles en ligne. Les personnes, les organisations et les États-nations tirent de plus en plus parti de ces vulnérabilités pour copier illégalement des propriétés intellectuelles afin de promouvoir leurs intérêts économiques, se saisir de renseignements personnels identifiables pour les revendre sur le marché noir et dérober des recherches universitaires en vue de servir des intérêts souverains, voler de l'argent ou des cryptomonnaies pour contourner les répercussions de sanctions et semer la méfiance entre les partis politiques, les dirigeants et les pays. À titre de témoignage de l'anxiété provoquée par les cyberhostilités interétatiques, les États-Unis et le Royaume-Uni ont, en 2018, pris la mesure historique d'avertir ensemble un autre État que la Russie s'était infiltrée dans son infrastructure énergétique et de transport, dans ses installations nucléaires ainsi que dans les systèmes d'entreprises privées revêtant une importance tout aussi cruciale (ministère de la Sécurité intérieure des É.-U., 2018).

Une foule d'institutions multilatérales font de la sensibilisation concernant l'utilisation responsable de la technologie et réclament un comportement normatif ou « responsable » entre les nations. La conclusion d'un accord international définissant les comportements acceptables et inacceptables dans l'espace cybernétique constitue une priorité pour presque tous les pays qui cherchent à instaurer la stabilité et la sécurité dans l'espace cybernétique (Finnemore et Hollis, 2016; Henriksen, 2019). La première série de discussions à cet égard a été proposée par la Russie en 1998. Le Secrétaire général de l'ONU a créé un Groupe d'experts gouvernementaux (GEG) chargé d'étudier l'évolution du domaine de l'information et des télécommunications dans le contexte de la sécurité internationale »[2]. Depuis 2004, cinq GEG ont continué d'étudier les menaces posées par l'utilisation abusive des technologies de l'information et des communications (TIC) dans le contexte de la sécurité internationale ainsi que la façon de remédier à ces menaces. Trois de ces groupes se sont accordés sur des rapports de fond assortis de conclusions et de recommandations[3].

En juillet 2015, des pays membres du GEG de l'ONU ont approuvé et adopté une nouvelle série de normes volontaires non contraignantes de comportement étatique responsable dans l'espace cybernétique. Selon l'une des normes les plus importantes acceptées par ce groupe, un État ne doit pas effectuer ou appuyer sciemment une activité de TIC qui contrevient à ses obligations en vertu du droit international, endommage intentionnellement des infrastructures essentielles ou gêne l'utilisation et l'exploitation d'infrastructures essentielles servant à offrir des services au public (Assemblée générale de l'ONU, 2015, par. 13[f]). Cependant, comme l'ont montré l'incident de WannaCry (attribué à la Corée du Nord), l'attaque destructive de NotPetya (attribuée à la Russie) et d'autres attaques similaires contre des entreprises et des pays, les mesures prises par les États ne correspondent souvent pas aux idéaux qu'ils professent, et les normes de conduite sont régulièrement ignorées (Hathaway, 2017, 2). L'endommagement intentionnel de l'infrastructure d'autres nations est en train de devenir tacitement acceptée comme une chose normale.

En septembre 2017, le Secrétaire général de l'ONU, António Guterres, a affirmé que la guerre cybernétique était en train de devenir une réalité de moins en moins dissimulée et de plus en plus capable de perturber les relations entre les États et de détruire certaines structures et certains systèmes de la vie moderne (Secrétaire général de l'ONU, 2017). Il a reconnu que les formes de réglementations traditionnelles ne s'appliquaient pas, d'où la nécessité d'une vision stratégique, d'une réflexion éthique et d'une réglementation judicieuse (ibid.). Lors de la réunion plénière de l'Assemblée générale de l'ONU de décembre 2018, on a lancé deux processus pour discuter du problème de la sécurité dans le milieu des TIC pour la période de 2019 à 2021. La Résolution 73/27 proposée par la délégation russe a établi un Groupe de travail à composition non limitée formé de tous les membres de l'ONU (Assemblée générale de l'ONU, 2018a; 2018b). Les membres de ce groupe continueront de développer des normes et des principes visant à promouvoir le comportement responsable des États dans l'espace cybernétique et chercheront des moyens de les mettre en œuvre. Ils présenteront un rapport final lors de la soixante-quinzième session de l'Assemblée générale de l'ONU, en septembre 2020. Une autre résolution, proposée par les États-Unis, a donné lieu à la création d'un nouveau GEG sur la promotion du comportement responsable des États dans l'espace cybernétique dans le contexte de la sécurité internationale (Assemblée générale de l'ONU, 2019). Ce groupe continuera d'étudier les mesures de coopération possibles visant à remédier aux menaces à la sécurité de l'information.

D'autres organisations internationales se sont aussi employées à promouvoir l'utilisation responsable de la technologie afin de renforcer la confiance dans l'utilisation des TIC et de réduire au maximum les méfaits cybernétiques. Les 57 États membres de l'Organisation pour la sécurité et la coopération en Europe (OSCE) ont, par exemple, adopté 16 mesures de renforcement de la confiance (MRC) pour diminuer les risques de conflit découlant de l'utilisation abusive des TIC et accroître la coopération entre les États afin de protéger les infrastructures essentielles. L'OSCE pense que l'intensification d'une communication directe entre les États permettra de désamorcer les conflits et d'empêcher l'escalade involontaire de la discorde. Bien que ce document soit rédigé sous la forme d'un accord non contraignant, il permet de faire progresser la coopération internationale dans l'espace cybernétique afin de promouvoir des pratiques exemplaires et de remédier à des vulnérabilités qui affaiblissent notre économie. D'autres institutions multilatérales ont adopté ces MRC, notamment l'Organisation des États américains et l'Association des Nations de l'Asie du Sud-Est.

Cependant, parallèlement à ces efforts normatifs et propices à l'instauration de la confiance, les pays développent également leurs propres capacités offensives pour empêcher les attaques cybernétiques ou y remédier. Le problème est qu'ils jouent avec le feu. Par exemple, au Sommet de l'Organisation du traité de l'Atlantique-Nord (OTAN) de Varsovie, en 2016, les membres de l'Alliance ont déclaré que le cyberespace constituait le cinquième domaine de guerre. Depuis ce moment-là, sept membres se sont

En 2016, au Sommet de l'OTAN de Varsovie, les membres de l'Alliance ont déclaré que l'espace cybernétique constituait le cinquième domaine de guerre. Depuis ce moment-là, sept membres se sont engagés à consacrer leurs armes cybernétiques offensives à l'Alliance et à se tenir prêts à aider les autres membres en cas d'attaque cybernétique grave. (Photo : Drop of Light / Shutterstock.com)

engagés à consacrer leurs armes cybernétiques offensives à l'Alliance et à employer toute la force de leur arsenal si l'un des membres était victime d'une attaque cybernétique particulièrement grave.[4] À partir de maintenant, l'OTAN intégrera les effets souverains des nations capables de les offrir et disposées à le faire (Freedberg, 2018).

Le rôle de la gouvernance dans la réduction des risques cybernétiques

L'environnement numérique continue d'inonder nos maisons, nos entreprises et nos pays de produits et de services pré-emballés assortis de faiblesses exploitables. Les incidents très médiatisés touchant la sécurité cybernétique de ces dernières années témoignent d'une attitude qui continue de dominer le développement et la commercialisation des technologies numériques : les entreprises tentent par tous les moyens d'offrir des produits le plus rapidement possible et ne se soucient des lacunes liées à la sécurité qu'après le lancement du produit. En fin de compte, le paradigme du « lancement maintenant, correction en suite », qui continue de prévaloir dans l'industrie de la technologie, doit être surmonté. Si nous voulons bénéficier d'un degré plus élevé de sécurité ou, du moins, diminuer considérablement les risques cybernétiques liés à l'ère numérique, il faut que les gouvernements interviennent et obligent les fournisseurs de services numériques ainsi que les fabricants de technologies des TIC à rendre des comptes de façon à ce que leurs produits respectent des normes de cybersécurité adéquates.

Au fur et à mesure que cette menace est devenue de plus en plus évidente, les gouvernements du monde entier ont commencé à élaborer des cadres de travail afin de saisir la nature de leur dépendance numérique, les stratégies de cybersécurité visant à éradiquer ces menaces et les politiques servant à établir des normes de comportement sécuritaire.

Par exemple, aux États-Unis, le ministère du Commerce lance actuellement une initiative afin d'améliorer la transparence des composantes logicielles. Ce projet de loi sur le matériel logiciel, connu sous le nom de Software Bill of Materials, sert à mettre en place un processus de divulgation visant à inciter les fournisseurs de logiciels et d'IoT à partager avec leurs clients les détails des composantes, des bibliothèques et des dépendances sous-jacentes de leur logiciel. Selon Allan Friedman, directeur de la cybersécurité de l'administration nationale des télécommunications et de l'information, cette transparence peut catalyser un marché plus efficace pour la sécurité afin de permettre aux fournisseurs d'établir une qualité de signaux et de donner aux clients des entreprises des connaissances clés : on ne peut pas défendre ce que l'on ne connaît pas (Friedman, cité dans Epper Hoffman, 2018). Elle permettrait aussi aux entreprises de mieux connaître les risques inhérents à leurs affaires numériques (i.e., *patch Tuesday*).

Si cette initiative ne catalyse pas les acteurs de l'industrie pour les inciter à prendre plus de responsabilités concernant les lacunes intrinsèques de leurs produits, l'État de la Californie a adopté une approche encore plus proactive : en prévision du déploiement des vulnérabilités de l'IoT, cet État a adopté une loi sur les appareils connectés qui établit les caractéristiques de sécurité devant être incluses à tous les appareils numériques connectés[5]. Cette loi entrera en vigueur le 1er janvier 2020. Elle exige des fournisseurs qui ont l'intention de vendre des appareils connectés (i.e., IoT) en Californie qu'ils mettent en place des mesures de sécurité renforcées pour tous ces produits. Elle définit les appareils comme tout appareil qui se connecte *directement ou indirectement* à l'Internet et comporte un protocole Internet ou une adresse Bluetooth. Ces mesures de sécurité comprennent des attestations d'appareil, une signature de code et une vérification de sécurité pour les microgiciels des composantes de niveau inférieur.

En Europe, le Règlement général sur la protection des données (Conseil de l'Union européenne, 2016), qui est entré en vigueur en mai 2018, a pour objectif de rendre les entreprises responsables de la sécurité numérique des renseignements personnels. La Directive sur la sécurité du réseau et de l'information établit des normes minimales pour la cybersécurité des infrastructures essentielles, dont celles qui touchent l'énergie, le transport, les affaires bancaires, les finances, la santé, l'eau et les infrastructures numériques, telles que les marchés en ligne (par exemple, eBay et Amazon), les moteurs de recherche (par exemple, Google) et les nuages. Les entreprises victimes d'une intrusion ou d'une interruption de service majeure doivent aviser les autorités nationales pertinentes dans les 48 heures et indiquer les données suivantes : la durée de l'incident, le nombre de parties touchées (par ex., clients, fournisseurs, etc.), l'étendue géographique, l'ampleur de la perturbation du service et les répercussions sur les activités sociétales et économiques (calculées en termes de PIB)[6].

De même, la Chine a adopté une loi nationale sur la cybersécurité, qui est entrée en vigueur en juin 2017. Cette loi contient 79 articles différents qui exposent en détails les exigences de protection des données et les directives sur la circulation transfrontalière des données applicables aux « infrastructures d'information essentielles » (IIE). Ces infrastructures comprennent les services d'information, et la loi établit une vaste définition des IIE selon laquelle elles constituent un service dont la destruction, la perte de fonctionnalité ou la fuite de données est susceptible de porter gravement atteinte à la sécurité nationale, à l'économie nationale et à l'intérêt public (Creemers, Triolo et Webster, 2018).
Le fil commun entre ces politiques est que les activités cybernétiques destructrices et perturbatrices nécessitent une attention et des mesures urgentes. Quelles que soient leur ampleur et leur portée, les stratégies nationales de cybersécurité échoueront en l'absence d'une hiérarchie des responsabilités claire qui détermine les obligations de sécurité incombant à chaque partie. Actuellement, la délégation des tâches entre le gouvernement et le secteur privé demeure floue dans de nombreux domaines, dont celui de la protection des infrastructures essentielles. Cette ambiguïté fait qu'il est particulièrement difficile de tenir les organisations responsables du laxisme des normes de sécurité. Il sera nécessaire d'effectuer des évaluations globales et méthodiques des risques cybernétiques au niveau national pour cerner correctement les principaux domaines de vulnérabilité et remédier aux lacunes des stratégies de défensives actuelles. Les décideurs doivent établir les risques qu'ils sont disposés à prendre et ceux qu'ils considéreraient comme intolérables. Les activités de réduction du risque requièrent également l'allocation des ressources, financières et humaines, suffisantes et appropriées à leur réalisation. Ce n'est qu'avec les efforts concertés et coordonnés de tous les intervenants à l'échelle nationale qu'il sera possible de réduire considérablement les risques cybernétiques et d'aller de l'avant pour assurer la sécurité future d'une nation.

Les gouvernements font face à des manques de ressources et devront s'adonner à une réflexion sincère et honnête pour fixer des priorités concernant la sécurité numérique. Bon nombre des approches politiques actuelles ratissent large lorsqu'il s'agit de déterminer les systèmes jugés essentiels à la sécurité nationale et économique.

Ce faisant, les pays risquent, cependant, de consacrer trop peu d'attention et de ressources aux quelques infrastructures, services, entreprises et actifs desquels tout le reste dépend. Or, la réalité est que certains d'entre eux sont plus importants que d'autres. Par exemple, l'approvisionnement en énergie et en télécommunications est essentiel à la santé économique et à la sécurité nationale au niveau le plus fondamental, car presque tous les autres systèmes cesseraient de fonctionner sans eux. Certaines entreprises responsables d'une grande proportion de l'économie totale d'un pays peuvent également exiger une attention spéciale. Par exemple, A.P. Moller-Maersk contribue à une grande partie du PIB du Danemark, de sorte que lorsque, l'entreprise a été victime de NotPetya en 2017, l'économie danoise a subi des dommages collatéraux considérables. Les États-Unis et l'Allemagne ont procédé en identifiant les entreprises qui contribuaient à hauteur de plus de 2 % au PIB national et en concluant avec elles de meilleurs accords de partage de l'information pour veiller à ce que les problèmes de cybersécurité soient dûment pris en considération dans le cadre des mesures de protection corporatives (Hathaway, 2018, 9).

En dépit d'un accord presqu'universel concernant l'importance de protéger intensivement des services et des biens essentiels des méfaits cybernétiques, les gouvernements ont jusqu'ici eu de la difficulté à évaluer avec précision où se trouvent les principales vulnérabilités et ainsi à déterminer ce qui nécessite leur attention immédiate, ou la principale priorité. Par exemple, la ville d'Atlanta, l'une des cent villes les plus

Les vulnérabilités du système d'exploitation de Windows ont été dévoilées par des pirates qui avaient obtenu un accès non autorisé à une base de données interne de Microsoft en 2013. (Photo : RoSonic / Shutterstock.com)

Chaque vulnérabilité est à un clic de se faire exploiter à l'aide d'armes et de services abordables et facilement accessibles en ligne.

résilientes de la planète, a été mise hors ligne en mars 2018 par le raçongiciel SamSam (Schwartz, 2018). Suite à la vérification de janvier 2019, on a constaté que le système de sécurité de la ville comportait des lacunes auxquelles on n'avait pas remédié. Moins de six mois plus tard, un autre bien essentiel des États-Unis, le port de San Diego, a subi l'attaque d'un rançongiciel issu de la même variante de logiciel malveillant que celui utilisé à Atlanta. SamSam a affecté des systèmes de TI et perturbé des services publics (Kan, 2018). Aux Pays-Bas, en dépit des efforts consentis par le gouvernement hollandais pour renforcer la cybersécurité de ses infrastructures et services essentiels, les fonctionnaires ont été pris de court lorsque le port de Rotterdam (le plus grand d'Europe) a été victime du logiciel malveillant NotPetya en 2017. Suite à d'autres examens, des fonctionnaires hollandais ont découvert qu'ils n'avaient pas classé les ports dans les infrastructures essentielles lors de l'élaboration de leurs politiques de protection des infrastructures (Hathaway, 2018). Bon nombre de biens essentiels à la vitalité économique et à la sécurité nationale ont été omis par les stratégies de cybersécurité actuelles, ce qui nécessite des évaluations plus rigoureuses à l'échelle du pays.

Il est temps de prendre des mesures stratégiques

En l'état actuel des choses, les pays à l'avant-garde des limites de la technologie progressent à un train d'enfer dans le développement et le déploiement de l'IoT et d'autres technologies novatrices. Les avantages des pionniers en la matière semblent tellement grands que la majorité des acteurs concernés ne prennent pas le temps de tenir compte des effets potentiellement déstabilisants de ces technologies par crainte de prendre du retard sur leurs concurrents économiques et géopolitiques. Or, en obtenant un avantage dans ce « bras de fer technologique », les pays deviennent plus dépendants de technologies de plus en plus complexes et opaques, et ainsi de plus en plus vulnérables, ce qui entraîne un risque plus élevé d'accidents et d'effets négatifs imprévus. Comme les auteurs d'un récent rapport du Center for a New American Security l'affirment : la supériorité n'est pas synonyme de sécurité (Danzig, 2018, 7). À long terme, ce seront les nations qui auront pris le temps d'envisager les possibilités d'utilisation antagoniste des technologies qui seront les mieux placées pour récolter des fruits en termes de richesse et d'influence.

Un accroissement de l'automatisation, de l'interconnectivité et de la dépendance à l'Internet nous contraint d'accueillir une nouvelle forme de coopération, au sein de laquelle les vulnérabilités sont communiquées au propriétaire du système d'information, ce qui donne à l'organisation concernée la possibilité de diagnostiquer la vulnérabilité en question et d'y remédier avant que des renseignements détaillés à son sujet ne soient divulgués à des tiers ou au public. Ce processus est connu sous le nom de divulgation responsable. Idéalement, on peut empêcher en grande partie les vulnérabilités à l'aide d'un processus de conception qui accorde une plus grande priorité à la sécurité. Jusqu'ici, l'industrie des TIC a emprunté un chemin différent et de nombreuses vulnérabilités ne sont réparées qu'après l'intégration d'un produit dans un environnement opérationnel et des systèmes de soutien essentiels (Internet Engineering Task Force, 2002).

Les États-Unis maintiennent une base de données nationale sur les vulnérabilités; 78 organisations de 14 pays utilisent ces données. Les vulnérabilités transmises par l'équipe de préparation aux urgences informatiques à l'agence de la sécurité des infrastructures cybernétiques du ministère de la Sécurité intérieure sont divulguées au public dans les 45 jours suivant le rapport initial, quels que soient les solutions ou les correctifs existants ou offerts par les fournisseurs concernés. La Chine a un système similaire, mais il fonctionne deux fois plus vite, soit 13 jours après la divulgation publique, en moyenne. La Chine écume proactivement le Web et d'autres sources d'information à la recherche de renseignements sur des vulnérabilités, tandis que les États-Unis attendent que les rapports des fournisseurs soient traités par la base de données des expositions et des vulnérabilités courantes (Waterman, 2017).

Le compromis entre la divulgation rapide et le refus de publier les vulnérabilités pendant un certain temps peut avoir des conséquences majeures. Du point de vue d'un gouvernement, la divulgation d'une vulnérabilité peut signifier que des organismes de renseignement manquent une occasion de recueillir des renseignements essentiels susceptibles de contrecarrer une attaque terroriste, de stopper le vol de la propriété intellectuelle d'une nation ou même de découvrir des vulnérabilités encore plus dangereuses utilisées par des pirates ou d'autres adversaires pour exploiter les réseaux gouvernementaux (la Maison-Blanche, 2014). Cependant, doit-on considérer qu'il est acceptable qu'une entreprise décide de ne pas divulguer des vulnérabilités critiques non résolues de son logiciel? Que penser lorsque la base de données de toutes les vulnérabilités connues est illégalement copiée par des acteurs malveillants? Y-a-t-il une obligation de divulguer la perte et de commencer à remédier au risque que l'entreprise a dorénavant transféré à la société? En 2013, des pirates ont obtenu un accès non autorisé à une base de données de Microsoft qui contenait la description de vulnérabilités logicielles critiques et non résolues concernant, entre autres, le système d'exploitation de Windows (Menn, 2017). En août 2016, des outils gouvernementaux essentiellement axés sur l'exploitation de ces vulnérabilités de Microsoft ont commencé à être publiés, et à constituer une menace réelle pour les entreprises du monde entier et l'économie mondiale. Certains de ces outils (comparables à des armes) ont été à l'origine des attaques de WannaCry et de NotPetya en 2017 (Patel, 2017; Hay Newman, 2017; Schneier, 2017).

En février 2017, Microsoft a lancé une campagne pour détourner l'attention des lacunes de ses produits et a mis la responsabilité de l'exploitation de ces vulnérabilités sur le dos des États. Elle a lancé sa campagne sur la « Convention numérique de Genève » en déclarant que les gouvernements devraient s'engager à protéger les civils des attaques des États-nations en temps de paix. Les auteurs du document affirment qu'à l'instar de la quatrième Convention de Genève, qui reconnait que la protection des civils nécessite l'intervention active de la Croix-Rouge, la protection contre les cyberattaques d'États-nations requière l'aide active des entreprises technologiques. Selon Microsoft, le secteur technologique joue un rôle unique en tant qu'intervenant de première ligne sur l'Internet et, pour cette raison, les entreprises technologiques doivent s'engager à prendre des mesures collectives qui rendront l'Internet plus sécuritaire en jouant le rôle d'une « Suisse numérique » neutre qui aide ses clients partout sur la planète et conserve la confiance du monde (Smith, 2017). Il est, cependant, dommage que cette entreprise ait choisi de chercher à conclure une convention sur la normalisation du comportement étatique afin de remédier aux lacunes de ses propres produits. Microsoft a poursuivi sur sa lancée pour préconiser un accord technologique sur la cybersécurité, lancé en 2018, qui promet de défendre et de faire progresser les avantages des TIC pour la société. Cet accord part du principe que les entreprises technologiques sont les héritières légitimes qui créent et exploitent des technologies en ligne. Finalement, les efforts de Microsoft ont à nouveau été mis en lumière dans l'Appel de Paris pour la confiance et la sécurité dans l'espace cybernétique annoncé lors de l'ouverture du Forum sur la Gouvernance d'Internet en novembre 2018. Cet appel a été appuyé par des gouvernements et des organisations du secteur privé du monde entier. Mais, dans quelle mesure devons-nous croire le charlatan qui dissimule sa négligence et rejette la responsabilité sur le dos d'une autre partie? La société a besoin de chefs d'entreprise éthiques et sérieux déterminés à instaurer un avenir numérique caractérisé par la résilience et la sécurité pour tous (Tech Accord, 2019).

Nous devons envisager de façon beaucoup plus stratégique la façon dont les nouvelles technologies numériques sont créées et déployées. Au cours des 30 dernières années, nous avons produit une vulnérabilité unique et stratégique pour la société : un Internet intrinsèquement non sécuritaire soutenu par des produits mal conçus. Cet Internet représente une menace existentielle pour notre économie et la sécurité de notre souveraineté. Pour remédier à cette menace immédiate, il faut mettre en place un processus d'atténuation et un conseil mondial chargé d'élaborer des contre-mesures d'urgence et constitué des meilleurs talents, quelle que soit leur nationalité. L'industrie a rapidement mis en marché des produits vulnérables; nous devons unir nos forces pour en diminuer les risques et restaurer notre environnement numérique le plus rapidement possible.

Nos gouvernements doivent exiger : un nouveau processus de divulgation des vulnérabilités (assorti de conditions d'exploitation), une obligation d'avertissement face à un danger imminent, par ex., lors d'une attaque émergente, et une obligation de porter assistance en cas d'urgence cybernétique (Hathaway et Savage, 2012). Il faut exiger des fournisseurs de produits des TIC qu'ils mettent en place un nouveau système de communication et de mise en garde pour les correctifs urgents, et ajoutent « urgent » à leur répertoire de catégories (urgent, critique, important, moyen et bas).

Les organismes de protection des consommateurs doivent aussi mettre la main à la pâte. Nous avons l'habitude des rappels d'aliments, de médicaments, d'automobiles, et même de jouets pour enfants; or, les produits de TI ne font pas l'objet de rappel, même lorsqu'on sait qu'ils peuvent causer de graves préjudices à la société. Les organismes de protection des consommateurs peuvent favoriser la responsabilisation en éliminant ou en réduisant

considérablement les réparations subséquentes à la mise en marché (*patch Tuesday*) par l'instauration d'un marché propice à la responsabilisation grâce au rappel de produits. Les fournisseurs devraient être tenus d'offrir des produits et des services bien conçus et présenter à l'acheteur une liste des composantes, des bibliothèques et des dépendances sous-jacentes, une sorte de liste du matériel, afin de promouvoir la transparence et la responsabilisation. Ce processus pourrait aussi éclairer les révisions émergentes de la norme ISO/IEC 29147:2014 sur les technologies de l'information et de la sécurité et la divulgation des vulnérabilités[7].

Finalement, l'Assemblée générale de l'ONU a reconnu l'importance de réduire la menace que représentent les TIC pour la société en lançant deux nouveaux fora visant à délibérer de la normalisation des comportements étatiques et à élaborer de réelles mesures de coopération afin de remédier aux menaces posées à la sécurité de l'information. Ces efforts sont essentiels pour développer des voies de communication directes entre les États ainsi que pour aider à prévenir l'escalade involontaire de la discorde dans l'espace cybernétique.

Ces dernières années, le monde a été témoin d'un nombre alarmant de pratiques nuisibles dans le domaine des TIC et d'actes internationalement répréhensibles issus de l'utilisation abusive des TIC. Nous avons mis un degré de foi immense, peut-être injustifié, dans les nouvelles technologies. Nous avons tendance à être certains que la technologie fonctionnera toujours comme prévu et seulement dans le but prévu, souvent sans nous préoccuper de la façon dont ces technologies créées pour résoudre nos problèmes pourraient servir à des fins malveillantes. Le temps est venu de reconnaître la prépondérance de ce problème et de soumettre le développement technologique à une surveillance accrue. Parallèlement aux avantages potentiels des nouvelles technologies, il faut aussi tenir compte de leurs défauts. Ce n'est qu'à ce moment-là que nous pourrons commencer à éradiquer les vulnérabilités du cœur de notre avenir numérique.

Ouvrages cités

A.P. Moller-Maersk. 2016. *Annual Report 2016*. http://investor.maersk.com/static-files/a31c7bbc-577a-49df-9214-aef2d649a9f5.

———. 2017. *Annual Report 2017*. http://investor.maersk.com/news-releases/news-release-details/annual-report-2017.

Ashford Warwick. 2019. « Norsk Hydro urges caution as it counts cost of cyber attack ». *Computer Weekly*, le 3 mai. www.computerweekly.com/news/252462778/Norsk-Hydro-urges-caution-as-it-counts-cost-of-cyber-attack.

Barysevich Andrei. 2017. « Dissecting the Costs of Cybercriminal Operations ». *Recorded Future* (blogue), le 2 novembre. www.recordedfuture.com/cyber-operations-cost/.

Cleo. 2018. « 10 Mind-Boggling Figures that Describe the Internet of Things (IoT) ». Cleo, le 4 juin. www.cleo.com/blog/internet-of-things-by-the-numbers.

Conseil de l'Union européenne. 2016. « Règlement général sur la protection des données (UE 5419/16) ». Le 6 avril. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

Creemers Rogier, Paul Triolo et Graham Webster. 2018. « Traduction : Cybersecurity Law of the People's Republic of China (en vigueur à partir du 1er juin 2017) ». *New America*, le 29 juin.

Danzig Richard. 2018. « Technology Roulette: Managing Loss of Control as Militaries Pursue Technological Superiority ». Center for a New American Security, le 30 mai. www.cnas.org/publications/reports/technology-roulette.

Dell SecureWorks. 2016. « Underground Hacker Markets: Annual Report ». Avril. http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf.

Desruisseaux Daniel. 2018. « Cyber-Nationalism in Cybersecurity Standards ». *Schneider Electric Blog*, le 16 avril. https://blog.schneider-electric.com/cyber-security/2018/04/16/cyber-nationalism-in-cybersecurity-standards/.

Epper Hoffman Karen. 2018. « Assembling an Ingredients List for Software ». GCN,le 24 août. https://gcn.com/articles/2018/08/24/software-bill-of-materials.aspx.

Federal Bureau of Investigation. 2017. « Internet Crime Report. » https://pdf.ic3.gov/2017_IC3Report.pdf.

Finnemore Martha et Duncan Hollis. 2016. « Constructing Norms for Global Cybersecurity ». *The American Journal of International Law* 110 (3): 425–79.

Franceschi-Bicchierai Lorenzo. 2019. « Ransomware Forces Two Chemical Companies to Order 'Hundreds of New Computers ». Mother Board, le 23 mars. https://motherboard.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers.

Freedberg Sydney. 2018. « NATO To 'Integrate' Offensive Cyber By Members ». Breaking Defense, le 16 novembre. https://breakingdefense.com/2018/11/nato-will-integrate-offensive-cyber-by-member-states/.

Giles Martin. 2019. « Triton is the World's Most Murderous Malware, and it's Spreading ». *MIT Technology Review*. Le 5 mars. www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/?utm_campaign=the_download.unpaid.engagement&utm_source=hs_email&utm_medium=email&utm_content=70515982&_hsenc=p2ANqtz--8Fah3uvccriLrQKjSj0SjFR3EPnEVAoenlpcLTS__xyEmUD-5a6zRbhGHrLBRDWBzCToBjwYpdONbwcfiCCbyRmDJxrRD83KKxWdtbwfqB8Wg9UY&_hsmi=70515982.

Greenberg Andy. 2018. « The Untold Story of NotPetya, the Most Devastating Cyberattack in History ». *Wired*, le 22 août. www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hathaway Melissa. 2012. « Falling Prey to Cybercrime: Implications for Business and the Economy ». Tiré de *Securing Cyberspace: A New Domain for National Security*, édité par Nicholas Burns et Jonathon Price, 145–57. Aspen, CO: The Aspen Institute.

———. 2017. *Getting Beyond Norms: When Violating the Agreement Becomes Customary Practice*. CIGI Paper n° 127. Waterloo, ON: CIGI. www.cigionline.org/publications/getting-beyond-norms-when-violating-agreement-becomes-customary-practice.

———. 2018. « Managing National Cyber Risk ». Organization of American States. White Paper Series, Issue 2. www.oas.org/es/sms/cicte/ENGcyberrisk.pdf.

Hathaway Melissa et John E. Savage. 2012. « Duties for Internet Service Providers ». Document présenté au Cyber Dialogue de 2012. Centre canadien des études sur la sécurité mondiale, Munk School of Global Affairs, Université de Toronto, mars.

Hay Newman Lyli. 2017. « The biggest cybersecurity disaster of 2017 so far ». *WIRED*, le 1er juillet. www.wired.com/story/2017-biggest-hacks-so-far/.

Henriksen Anders. 2019. « The end of the road for the UN GGE process: The future regulation of cyberspace ». *Journal of Cybersecurity* 5 (1). https://doi.org/10.1093/cybsec/tyy009.

Hill Kashmir. 2013. « The Crazy Things a Savvy Shodan Searcher Can Find Exposed on the Internet » *Forbes*, le 5 septembre. www.forbes.com/sites/kashmirhill/2013/09/05/the-crazy-things-a-savvy-shodan-searcher-can-find-exposed-on-the-internet/#510502793c7e.

Huawei and Oxford Economics. 2017. « Digital Spillover: Measuring the true impact of the digital economy ». Le 5 septembre. www.huawei.com/minisite/gci/en/digital-spillover/files/gci_digital_spillover.pdf.

Internet Engineering Task Force. 2002. « Responsible Vulnerability Disclosure Process ». Février. https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00.

Jackson Higgins Kelly. 2018. « Schneider Electric: TRITON/TRISIS Attack Used 0-Day Flaw in its Safety Controller System, and a RAT ». Dark Reading, le 18 janvier. www.darkreading.com/vulnerabilities---threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-in-its-safety-controller-system-and-a-rat/d/d-id/1330845.

Kan Michael. 2018. « Ransomware Strikes the Port of San Diego, Disabling IT Systems ». *PC Magazine*, le 28 septembre. www.pcmag.com/news/364081/ransomware-strikes-the-port-of-san-diego-disabling-it-syste.

Krebs Brian. 2019a. « Patch Tuesday Laydown, April 2019 ». *Krebs on Security* (blogue), le 9 avril. https://krebsonsecurity.com/2019/04/patch-tuesday-lowdown-april-2019-edition/.

———. 2019b. « Patch Tuesday Laydown, March 2019 ». *Krebs on Security* (blogue), le 19 mars. https://krebsonsecurity.com/2019/03/patch-tuesday-march-2019-edition/.

McCamy Laura. 2018. « 7 Things You Can Hire a Hacker to do, and How Much it will (Generally) Cost ». *Business Insider*, le 27 novembre. www.businessinsider.com/things-hire-hacker-to-do-how-much-it-costs-2018-11.

Menn Joseph. 2017. « Exclusive: Microsoft responded quietly after detecting secret database hack in 2013 ». Reuters, le 17 octobre. www.reuters.com/article/us-microsoft-cyber-insight/exclusive-microsoft-responded-quietly-after-detecting-secret-database-hack-in-2013-idUSKBN1CM0D0.

National Audit Office. 2017. « Investigation: WannaCry cyber attack and the NHS ». Le 27 octobre. www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

Office of the Director of National Intelligence. 2019. « National Intelligence Strategy of the United States of America ». www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.

Palmer Danny. 2019. « Ransomware: The Key Lesson Maersk Learned from Battling the NotPetya Attack ». ZD Net, le 29 avril.

Patel Andy. 2017. « Petya: 'I Want To Believe' ». *F-Secure* (blogue), le 29 juin. https://labsblog.f-secure.com/2017/06/29/petya-i-want-to-believe/.

Proviti. 2017. « How Long Does It Take to Implement a Patch? » Board Perspectives: Risk Oversight. Édition 97. www.protiviti.com/US-en/insights/bpro97.

Reuters. 2017. « Global Shipping Giant Maersk is Reeling from the Ransomware Fallout ». *Fortune*, le 29 juin. http://fortune.com/2017/06/29/petya-goldeneye-maersk-ransomware-effects/.

Schneier Bruce. 2017. « Who Are the Shadow Brokers? » *The Atlantic*, le 23 mai. www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

Schwartz Mathew. 2018. « Atlanta's Ransomware Cleanup Costs Hit $2.6 Million ». GovInfoSecurity, le 24 avril. www.govinfosecurity.com/atlantas-ransomware-cleanup-costs-hit-26-million-a-10888?rf=2018-04-25_ENEWS_SUB_GIS_Slot1&mkt_tok=e yJpIjoiWkRo aE16WXpNMkZo TmpJdyIsInQjOi JwMmJUS1pjcGRPcUZ oQ1RYc1VlXC8zbytua29UbUNKa2pqRT FwQ2ZqMXVoTUZWQXBhVVpPVUVVN1wvWHQ1WXJsT 3RFeUd1bXJGaG5CR2crenBvaTIzc1hxUU s2ZVl5ZmVtVkk3RytyNGhScldsaXpHYkp3am93TzdKcHZNU1BLQ3hcLyJ9.

Smith Brad. 2017. « The Need for a Digital Geneva Convention ». *Microsoft Blog*, le 14 février. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Sobczak Blake. 2019. « The inside story of the world's most dangerous malware ». E&E News, le 7 mars. www.eenews.net/stories/1060123327.

Symantec. 2018. *Internet Security Threat Report*. Volume 23. Mars. www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.

Tech Accord. 2019. « Reducing tensions in cyberspace by promoting cooperation. Cybersecurity Tech Accord publishes a set of recommendations on confidence-building measures in cyberspace ». Le 4 avril. https://cybertechaccord.org/reducing-tensions-in-cyberspace-by-promoting-cooperation-cybersecurity-tech-accord-publishes-a-set-of-recommendations-on-confidence-building-measures-in-cyberspace/.

La Maison-Blanche 2014. « Heartbleed: Understanding When We Disclose Cyber Vulnerabilities ». Le 28 avril. https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

Assemblée générale de l'ONU. 2015. « Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ». Le 22 juillet. https://undocs.org/A/70/174.

———. 2018a. « General Assembly Adopts 67 Disarmament Drafts, Calling for Greater Collective Action to Reduce Arsenals, Improve Trust amid Rising Global Tensions ». Communiqué, le 5 décembre. www.un.org/press/en/2018/ga12099.doc.htm.

———. 2018b. « Résolution adoptée par l'Assemblée générale le 5 décembre 2018 ». A/RES/73/27. Le 11 décembre. www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27.

———. 2019. « Résolution adoptée par l'Assemblée générale le 22 décembre 2018 ». A/RES/73/266. Le 2 janvier. www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266.

Secrétaire général de l'ONU. 2017. « Discours du secrétaire général à l'Assemblée générale ». Le 19 septembre.

Ministère de la Sécurité intérieure des É.-U. 2018. « Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors ». Le 15 mars. www.us-cert.gov/ncas/alerts/TA18-074A.

Vijayan Jai. 2017. « TRITON Attacker Disrupts ICS Operations, While Botching Attempt to Cause Physical Damage ». Dark Reading, le 14 décembre. www.darkreading.com/attacks-breaches/triton-attacker-disrupts-ics-operations-while-botching-attempt-to-cause-physical-damage-/d/d-id/1330650.

Waterman Shaun. 2017. « China's vulnerability disclosure system twice as fast as U.S. version ». CyberScoop, le 23 octobre. www.cyberscoop.com/china-vulnerability-reporting-nvd-recorded-future/.

Wladawsky-Berger Irving. 2017. « GDP Doesn't Work In A Digital Economy ». *The Wall Street Journal*, le 3 novembre. https://blogs.wsj.com/cio/2017/11/03/gdp-doesnt-work-in-a-digital-economy/.

Références

1 Le cours de l'action de Maersk a atteint un maximum d'environ 14 000 couronnes danoises juste avant l'attaque de NotPetya. Six mois après l'événement, il avait chuté à environ 10 000 couronnes danoises. Une année après l'incident, il avait encore chuté pour atteindre 8 000 couronnes danoises.

2 Voir www.un.org/disarmament/ict-security/.

3 Les rapports de fond des GEG de l'ONU comprennent : 2009/2010 – A/65/201; 2012/2013 – A/68/98*; 2014/2015 – A/70/174. Voir www.un.org/disarmament/ict-security/.

4 Les sept membres de l'OTAN qui se sont engagés à consacrer leurs armes cybernétiques offensives à l'Alliance sont l'Estonie, le Danemark, la France, l'Allemagne, les Pays-Bas, le Royaume-Uni et les États-Unis.

5 Voir https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

6 Voir https://eur-lex.europa.eu/eli/dir/2016/1148/oj et www.enisa.europa.eu/topics/nis-directive.

7 La révision de la norme internationale ISO/IEC DIS 29147 est actuellement en cours.