2018

White paper series
Édition 2

GÉRER LE RISQUE CYBERNÉTIQUE
— AU NIVEAU NATIONAL —

OEA | Plus de droits pour plus de personnes

CRÉDITS

Luis Almagro

Secrétaire général de
Organisation des États
Américains (OEA)

Auteur principal

Melissa Hathaway

Équipe technique de l'OEA

Claudia Paz y Paz
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Bárbara Marchiori de Assis
Nathalia Foditsch
Gonzalo Garcia-Belenguer

CONTENU

1

INTRODUCTION

Au cours des 30 dernières années, les gouvernements, les entreprises et les citoyens sont devenus extrêmement dépendants d'Internet et des technologies de l'information et de la communication (TIC). Nous supposons que les services essentiels aux citoyens comme l'électricité et les télécommunications, fonctionneront toujours et que les biens, les services, les données et le capital franchiront sans entrave les frontières. Toutefois, de nombreux systèmes et infrastructures en réseau sont vulnérables et exploités. Les organisations de tous types sont confrontées à une augmentation des violations de données, d'activités criminelles, de perturbation des services et de destruction de biens. L'insécurité augmente au niveau global. Plus de 100 pays ainsi qu'un nombre croissant d'acteurs non-étatiques et individus sont capables d'occasionner des dommages aux infrastructures gouvernementales et des entreprises. Les objectifs varient selon les acteurs. Ils vont de l'activisme politique et la fraude à la cybercriminalité, le vol de propriété intellectuelle (PI) l'espionnage, la perturbation des services et la destruction des biens et avoirs. Les pays et les entreprises vivent dans un monde de cyber insécurité. Les gouvernements, les industries et les particuliers font face à des risques cybernétiques et partagent un niveau de responsabilité dans leur gestion. Aux vues des événements récents, les pays et les entreprises doivent tout d'abord comprendre qu'une gestion des risques rigoureuse doit être l'élément central de leur stratégie et agenda numérique. Le risque d'inaction est trop important.

Le risque se défini en termes de temps lorsque quelque chose ou quelqu'un est exposé à un danger, un dommage ou une perte.[1] La condition d'occurrence du risque peut changer en fonction des mesures prises par au moins deux acteurs : l'attaquant, qui obtient et utilise les compétences permettant de causer des dommages puis, la cible visée, qui peut prendre des précautions pour résister ou contrecarrer le danger duquel elle est victime. Chaque jour, notre dépendance vis-à-vis du numérique augmente. Cependant, la compréhension des risques associés à cette dépendance demeure au stade embryonnaire. Pourtant, le cyber risque augmente car il existe un marché des logiciels et outils malveillants, des services illicites et des données sensibles (non publiques) disponible, abordable et utilisé. En effet, certains logiciels malveillants ne coûtent qu'un dollar et une attaque par déni de service distribué peut être lancée pour moins de mille dollars.[2] Des attaques sophistiquées par ransomware sont disponibles au prix de deux cents dollars et des services malveillants de courrier indésirable de messagerie électronique pour environ quatre cents dollars. Même les armes les plus sophistiquées des services de renseignement gouvernementaux peuvent être téléchargées.[3] Toute personne ayant l'intention de lancer et réussir une attaque malveillante peut accéder à ces capacités. Comme l'ont démontré les événements de 2017, les gouvernements, les entreprises et les individus ont été victimes de certaines des cyberattaques les plus importantes à ce jour.

En mai 2017, les ransomware ont ciblé les failles des systèmes d'exploitation Microsoft Windows, infectant des millions d'ordinateurs dans 150 pays et ont causé des dégâts dans tous les secteurs d'activité. Cette attaque mondiale, lancée avec un ransomware très simple appelé WannaCry, a provoqué l'arrêt des opérations de fabrication, des systèmes de transport et des systèmes de télécommunication. Selon le National Audit Office du Royaume-Uni, WannaCry a touché au moins 81 des 236 services de santé nationaux (National Health Service trusts), rendant le matériel médical inutilisable et affectant considérablement la santé et la sécurité publiques.[4]

En juin 2017, une attaque a été lancée avec un autre logiciel malveillant plus destructeur encore, baptisé NotPetya. Ce virus a touché les entreprises en réseau du monde entier à travers un mécanisme de mise à jour d'un logiciel de comptabilité largement utilisé à travers le monde (doc.me). En quelques minutes, le virus a infecté des dizaines de milliers de systèmes

connectés à Internet dans plus de 65 pays, y compris les systèmes appartenant à des institutions gouvernementales, des banques, des entreprises du secteur de l'énergie et d'autres sociétés. En effet, l'attaque NotPetya contre AP Moller-Maersk, la compagnie maritime la plus importante au monde, a crypté et effacé les systèmes informatiques de la société au niveau mondiale. À la suite de cette attaque, Maersk a dû interrompre ses activités dans la plupart de ses 76 terminaux portuaires à travers le monde, perturbant ainsi le commerce maritime pendant plusieurs semaines. Les pertes financières de Maersk dues à NotPetya ont dépassé les 300 millions de dollars. La société a dû reconstruire toute son infrastructure et investir dans l'achat de 4 000 nouveaux serveurs, 45 000 nouveaux ordinateurs et 2 500 nouvelles applications.[5] On estime que NotPetya a provoqué des milliards de dollars de pertes au niveau international par la perturbation des activités et la destruction de biens.[6] Les pertes des secteurs primaires et secondaires de l'économie numérique ont été importantes et il a fallu plusieurs mois pour se remettre des dommages causés aux services et infrastructures critiques.

Fait encore plus troublant, en août 2017, un complexe gazier et pétrolier saoudien a été soudainement contraint de fermer. Celui-ci a été victime de Trisis, un virus informatique sophistiqué conçu pour saboter les systèmes de contrôle industriels (ICS). Créé pour endommager les composants opérationnels des technologies de l'information sur des sites industriels tels que les complexes pétroliers, gaziers et des eaux, ce logiciel malveillant, ou arme, cible spécifiquement les mécanismes de sécurité physique (système d'arrêt d'urgence) du SCI. Bien que cela ne soit qu'un exemple de l'utilisation réussie de ce logiciel destructeur, Schneider Electric a demandé à ses clients de services critiques et aux propriétaires d'infrastructures de s'assurer que leurs systèmes soient redondants au cas où un ou plusieurs systèmes présenteraient des failles à la suite d'une attaque.[7]

En 2017, les activités cybernétiques malveillantes ont eu des conséquences inaccoutumées en termes de pertes et dommages. Néanmoins, les outils utilisés pour nuire étaient peu sophistiqués. Le nombre d'attaques ciblant les systèmes d'électricité, de télécommunication, de transport et financiers ont presque doublé au cours des cinq dernières années. Cette tendance présente un risque économique et sécuritaire pour tous au niveau national. Par conséquent, il est urgent que les leaders gouvernementaux et des entreprises s'engagent dans des processus efficaces de gestion des risques cybernétiques et puissent tenir compte des risques numériques dans leurs processus de planification stratégique.

2 CADRES POUR COMPRENDRE LES RISQUES CYBERNÉTIQUES

Les pays, les organisations internationales et les institutions universitaires élaborent des cadres pour aider la classe politique et les chefs d'entreprises à diagnostiquer et réduire les risques cybernétiques. Ces cadres sont nécessaires car au cours des trois dernières décennies, ces mêmes dirigeants ont été convaincus par les options et les « avantages » que présente l'informatique commerciale et tout particulièrement, par la possibilité d'une productivité accrue, une plus grande efficacité, des coûts d'équipement et de stockage moins élevés, le traitement des données et la croissance des bénéfices, et ont différé leurs investissements dans la sécurité et la résilience de leurs infrastructures en réseau et de leurs activités dans le domaine du numérique. Les activités cybernétiques destructrices et nuisibles que nous observons aujourd'hui exigent de ces dirigeants qu'ils reconnaissent avoir involontairement provoqué l'insécurité au sein de la société. Les pertes s'accumulent, le mal augmente et le danger est imminent.

Cadres gouvernementaux

Les gouvernements ont commencé à élaborer des cadres, des comparaisons et des stratégies nationales plus larges pour mieux comprendre leurs dépendances et leurs vulnérabilités face aux infrastructures d'Internet et pour sécuriser les réseaux, infrastructures et services nationaux dont dépendent leur avenir numérique et leur bien-être économique. Toutefois, lorsqu'il s'agit de cartographier et d'attirer l'attention sur le risque cybernétique encouru par un pays, la question qui demeure est la suivante : Comment diagnostiquer et réduire un risque qui s'est accumulé pendant 30 ans ?[8] Il est important de commencer par comprendre quel est le plan stratégique d'un pays sur 3 à 5 ans, puis déterminer ce qui peut être mis en œuvre pour atteindre cet objectif à plus long terme. Les Néerlandais ont ainsi estimé que d'ici 2020, l'économie numérique (soit les biens numériques et les services électroniques) représentera au moins 25% de leur produit intérieur brut (PIB). Les Pays-Bas ont affirmé que leur avenir dépendait de leur capacité à sécuriser leur économie numérique. Ils procèdent donc à réaliser les investissements indispensables et mener à bien les réformes structurelles nécessaires pour atteindre cet objectif. D'autres pays, tels que les États-Unis et l'Allemagne, identifient les principales entreprises, celles qui représentent plus de 2% du PIB de leur pays, et travaillent avec elles pour s'assurer que la gestion des risques et la résilience fassent partie intégrante de leurs processus de planification. Cependant, la grande majorité des autres pays ont opté pour une approche plus large, exigeant la protection des « infrastructures critiques », des actifs, systèmes et réseaux essentiels perçus comme étant particulièrement vulnérables en raison de l'interconnexion et la dépendance croissante à Internet qui, du fait de sa nature, peut présenter des défaillances, des erreurs, des pannes naturelles ou provoquées par les conditions climatiques, ou encore être la cible d'attaques physiques et cybernétiques.[9] Or, le problème de cette approche est qu'il n'existe pas de définition précise des responsabilités du gouvernement et de l'industrie. Il est donc particulièrement difficile de tenir quelqu'un responsable de toute inaction. En attendant, le sentiment d'insécurité de la société s'accroît face au manque d'engagement envers une réduction des risques et pour une augmentation de la résilience. Certains gouvernements ont déclaré qu'il était temps d'intervenir sur le marché et utilisent des règlements ou lois pour exiger que certains secteurs identifient, évaluent et corrigent les lacunes de leur système de sécurité. Les secteurs réglementés sont ceux des services d'électricité, des services financiers, des services de santé, des transports et des télécommunications. Les pays ont également adopté d'autres mesures réglementaires telles

que l'obligation de notifier en détail à l'autorité locale et/ou nationale : toute violation s'étant produite, ainsi que le type de données qui auraient été exposées ou perdues, la technique ou méthode utilisée pour commettre l'attaque et les pannes ou perturbations d'activité (télécommunications) qui se soient produites.

L'Union européenne (UE) impose ces types d'approches prescriptives aussi bien à leurs infrastructures critiques qu'à celles des opérateurs de services critiques. En août 2016, l'UE a adopté la Directive européenne sur la sécurité des réseaux et des systèmes d'information (NIS). Cette Directive établit des règles de cybersécurité, ou série de contrôles de sécurité, pour les entreprises fournissant des services considérés comme essentiels. Ce règlement s'applique aux secteurs de l'électricité, des transports, de la banque, de la finance, de l'eau et de la santé, ainsi qu'aux services numériques tels que les marchés en ligne (exemple : eBay, Amazon), les moteurs de recherche (Google) et les fournisseurs de services cloud. Les États membres de l'UE ont jusqu'à mai 2018 pour transposer ce texte dans leur droit national. La directive NIS exige que les opérateurs de services essentiels de ces pays prennent des mesures de sécurité appropriées et notifient aux autorités nationales (comme par exemple l'autorité compétente en la matière ou les équipes nationales d'intervention en cas d'incident contre la sécurité informatique) de tout incident cybernétique grave. Cette approche contraint à la responsabilisation et peut réduire les risques cybernétiques car elle « oblige » l'industrie à prendre des mesures pour réduire les vulnérabilités et accroître la résilience.

La Chine a adopté une approche semblable à celle de l'Europe et a même incorporé certains éléments de la directive NIS dans sa nouvelle loi nationale sur la cybersécurité, adoptée par le parlement chinois en novembre 2016 et entrée en vigueur le 31 décembre 2017. La loi comporte sept chapitres et 79 articles, et est considérée comme la « plus complète et la plus englobante » dans la mesure où elle spécifie les responsabilités des agences étatiques compétentes en la matière, des fournisseurs d'accès à Internet ainsi que des internautes. La loi précise que les entreprises, définies au sens large, devront mettre en place des mesures techniques et toute autre mesure nécessaire visant à assurer un fonctionnement sûr et stable d'Internet, gérer efficacement les incidents de cybersécurité, prévenir les activités cybercriminelles et maintenir l'intégrité, la confidentialité et la facilité d'utilisation des données Internet.[10] Ce règlement force les entreprises à investir dans de nouvelles protections et à mettre en place une série de contrôles pour garantir ces principes. Cette directive met également en place un régime d'inspection et d'audit pour s'assurer que les entreprises prennent des mesures appropriées en matière de réduction des risques et qu'elles soient tenues comme responsables au cas où les procédures mis en place soient jugées insuffisantes.

Les États-Unis se sont abstenus d'adopter une approche réglementaire dans ce domaine et ont plutôt fait appel à l'industrie pour qu'elle investisse de façon volontaire dans la réduction des risques cybernétiques des infrastructures et services critiques du pays. En février 2013, le président a demandé à l'Institut national des standards et de la technologie (NIST, National Institute of Standards and Technology). D'élaborer une série de normes, méthodologies, procédures et processus pour harmoniser les approches en matière politique, commerciale et technologique afin de lutter contre les risques cybernétiques. Le cadre pour l'amélioration de la cybersécurité des infrastructures critiques a été publié un an plus tard, en février 2014, et présente un ensemble de normes volontaires visant à aider les organisations à évaluer, gérer et faire face aux risques en matière de cybersécurité. Le cadre charge les organisations d'évaluer les risques sous cinq axes: identification, protection, détection, réponse et reprise. Selon certaines estimations, environ 30% des organisations américaines (y compris le gouvernement) utilisent ce cadre pour évaluer leur niveau de préparation face aux risques et se responsabiliser davantage dans la protection de leurs réseaux et leurs données sensibles contre toute intrusion, dommage ou destruction.[11] En outre, l'annexe de ce rapport établit une correspondance entre les différentes normes internationalement reconnues et les catégories de réduction des risques du Cadre de cybersécurité du NIST. Toutefois, aux vues des enseignements tirés face aux récentes violations, l'on constate que les organisations qui utilisent le cadre de cybersécurité du NIST, évaluent les catégories en vue de répondre à une exigence plutôt que pour mesurer le risque de façon continue. Ainsi, certaines organisations ont évalué leur niveau de sécurité et de préparation en utilisant le cadre de cybersécurité du NIST et ont estimé qu'elles avaient atteint un haut niveau de sécurité informatique, mais qu'elles étaient encore considérablement sensibles à WannaCry et NotPetya.[12]

En septembre 2017, le NIST a publié les révisions faites à une de ses publications sur le *Cadre de gestion des risques pour les systèmes d'information et les organisations : une approche axée sur le cycle de vie des systèmes pour la sécurité et la protection des données.*[13] Ce cadre recommande un processus permettant aux organisations d'identifier les actifs de grande valeur et les systèmes critiques afin qu'elles puissent mieux évaluer le risque opérationnel. Il fournit également une structure visant à déterminer et sélectionner les contrôles de sécurité et de confidentialité et à mettre en œuvre et évaluer l'efficacité de ces contrôles. Le cadre souligne l'importance d'un suivi permanent du risque en temps réel face à une conformité ponctuelle. Il reconnaît aussi que les décisions en matière de gestion des risques font partie intégrante des fonctions opérationnelles et de l'accomplissement de la mission. Ce cadre complète le *Cadre d'amélioration de la cybersécurité des infrastructures critiques* et, ensemble, peuvent fournir aux organisations une approche plus stratégique de la gestion des risques.

Cadres internationaux

Les organisations internationales expriment leurs opinions face au débat sur la gestion des risques cybernétiques et cherchent à accélérer l'adoption de mesures efficaces en matière de cybersécurité en utilisant leurs propres cadres et recommandations. Le débat international sur la gestion des risques a émergé après les deux phases consécutives (2003 et 2005) du Sommet mondial sur la société de l'information (SMSI), un rassemblement mondial de la communauté « TIC pour le développement ». À l'époque, 170 pays, au moins, s'étaient engagés à faire en sorte que tout le monde puisse bénéficier des opportunités offertes par les technologies de l'information et de la communication en améliorant l'accès aux infrastructures et aux TIC ainsi qu'à l'information et au savoir, en augmentant la confiance et la sécurité dans l'utilisation des TIC, en développant les applications TIC et en encourageant la coopération internationale et régionale.[14] À partir de ce moment, les institutions internationales se sont engagées à développer et diffuser des cadres visant à gérer les risques liés aux vulnérabilités des technologies de l'information et de la communication et accroître la confiance et la participation dans l'économie numérique mondiale.

L'Organisation des États américains (OEA) est l'une des premières organisations internationales à s'être engagée sue ce chemin. En 2004, l'OEA, par le biais du Comité interaméricain contre le terrorisme (CICTE) et son programme de cybersécurité, a encouragé le développement d'un programme de cybersécurité dans les Amériques. L'OEA coopère avec un large éventail d'entités nationales et régionales des secteurs public et privé sur les questions politiques et techniques et cherche à développer et renforcer les capacités des États membres en matière de cybersécurité grâce à une assistance technique, des formations, des tables rondes sur les politiques, des exercices de gestion de crise et un échange de meilleures pratiques dans le secteur des technologies de l'information et de la communication. L'OEA utilise des cadres gouvernementaux et académiques pour promouvoir le renforcement des capacités en matière de cybersécurité et contribue à modifier le dialogue nationale au sein de ses États membres afin qu'ils comprennent que la connexion Internet et l'infrastructure de TIC qui en découle, doit être sécurisée. Si les pays n'investissent pas de manière égale dans la sécurité de leurs infrastructures essentielles et dans la résilience de leurs systèmes, les coûts imposés par les cyberattaques auront un impact négatif sur leurs croissances économiques.

En 2007, l'Union internationale des télécommunications (UIT), une agence spécialisée des Nations Unies (ONU) chargée des questions sur les technologies de l'information et de la communication, a lancé le *Programme mondial de cybersécurité* (GCA) et a publié un cadre qui encourage la coopération et la collaboration entre les différentes parties prenantes. Le programme mondial de cybersécurité contient cinq piliers stratégiques permettant de guider les pays dans le renforcement de leurs capacités afin d'aborder la cybersécurité de manière responsable. Ces piliers sont les suivants : (1) mesures législatives; (2) mesures techniques et de procédure; (3) structures administratives; (4) renforcement des capacités et (5) coopération internationale. Par la suite, en 2011, ce cadre a conduit l'UIT à élaborer un guide de la cybersécurité national *(National Cybersecurity Strategy Guide)* qui met l'accent sur les valeurs, la culture et les intérêts nationaux comme fondements de toute stratégie nationale efficace. Ce guide aborde également des problématiques importantes auxquelles chaque gouvernement devrait s'attaquer lorsqu'il cherche à faire avancer le débat en matière de cybersécurité pour passer d'une vision de simple problème technique à une politique stratégique nationale. S'appuyant sur ces efforts initiaux, l'UIT a publié, en 2014, un Indice de cybersécurité dans le monde (GCI) en vue d'améliorer les données de référence des pays et évaluer leurs programmes de cybersécurité par rapport aux investissements et programmes réalisés dans d'autres pays. Cet indice mesure le niveau de développement ou « bien-être » de chaque pays suivant les cinq piliers du programme mondial de cybersécurité (GCA) : mesures législatives, mesures techniques et de procédure, structures administratives, renforcement des capacités et coopération internationale.[15] Cette méthodologie et cet indice ont constitué l'un des premiers cadres internationaux mis à la disposition des responsables nationaux. Ce cadre a permis d'obtenir des informations sur le développement des stratégies nationales et fournir une approche permettant de mesurer le risque cybernétique en termes non techniques.

En 2015, la *Recommandation sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale*[16] adopté et publié par le Conseil de l'Organisation de coopération et de développement économiques (OCDE) permet d'aider à l'élaboration de stratégies nationales visant à gérer la sécurité numérique et à optimiser les avantages économiques et sociaux escompté d'un plus grand accès au numérique. Ce cadre encourage les pays à adopter une approche fondée sur la gestion des risques et sur un ensemble de huit principes de haut niveau, indissociables, interdépendant et complémentaires : 1) la sensibilisation, l'acquisition de compétences et l'autonomisation; (2) la responsabilité des parties prenantes; (3) les droits de l'homme et les valeurs fondamentales; (4) la coopération; (5) l'évaluation des risques et le cycle de traitement; (6) les mesures de sécurité adaptées et proportionnelles au risque et à l'activité économique et sociale en jeu; (7) l'innovation et (8) la planification de la préparation et de la continuité des activités. Selon l'OCDE, si les responsables appliquent ces huit principes ainsi que d'autres cadres internationaux, les pays seraient en mesure de développer de meilleures politiques (et stratégies) articulées autour d'une gestion des risques en matière de sécurité numérique. Les huit principes ne constituent pas un cadre en soi. Il s'agit plutôt d'éléments clés permettant d'établir ou améliorer des mécanismes de coordination au sein du gouvernement et avec les parties prenantes non gouvernementales. L'OCDE reconnaît que la coopération entre les secteurs public et privé

est essentielle pour la réduction des risques cybernétiques.

En 2018, le Forum économique mondial (WEF) a publié le Cyber *Resilience Playbook for Public-Private Collaboration (Manuel de cyber-résilience pour la collaboration des secteurs public et privé)*[17] , un outil destiné à guider la collaboration public-privé intra-étatique sur l'élaboration de politiques en matière de cybersécurité. En effet, la section 4.7 du Manuel traite de la nécessité d'établir un cadre national précis en matière de cybergouvernance qui définisse les rôles, les responsabilités et les capacités attendus des secteurs public et privé. Le cadre proposé par le WEF se décompose en trois niveaux et cherche à aider les gouvernements nationaux dans l'attribution de responsabilités et à mieux aligner les rôles et responsabilités spécifiques avec les trois capacités de sécurité distinctes suivantes : la solidité, la résilience et la défense. Chacune renforçant les deux autres. La solidité se définie comme « la capacité à prévenir, repousser et contenir les menaces ». La résilience comme étant « la capacité à gérer des attaques réussies ». Et, la défense comme « la capacité d'anticiper, perturber et répondre aux attaques ».[18] Ce cadre s'inspire des initiatives remontant à l'agenda mondial 2014 sur le risque et la résilience du Conseil du Forum économique mondial et le livre blanc de 2016 intitulé *Comprendre le risque cybernétique systémique*. Le Forum économique mondial a réussi à encourager le débat sur le risque cybernétique et a mis en exergue les liens directs existant entre les impacts économiques et les conséquences commerciales de la cyber insécurité.

3 LES CADRES DES MILIEUX UNIVERSITAIRES ET DE LA COMMUNAUTÉ TECHNIQUE

Les institutions académiques, les groupes de réflexion et la communauté technique sont également des acteurs importants. Ils ont proposé diverses méthodologies pour accélérer la préparation et le degré de maturité des pays et des organisations face à la lutte contre la cybercriminalité.

L'Indice de préparation à la lutte contre la cybercriminalité version 2.0 (CRI 2.0)[19] , publié en 2015 par une équipe d'experts de l'Institut d'Études Politiques de Potomac, s'appuie sur l'Indice de préparation à la lutte contre la cybercriminalité version 1.0 de 2013 qui a fourni un cadre méthodologique pour l'évaluation de la préparation à la lutte contre la cybercriminalité. L'Indice de préparation à la lutte contre la cybercriminalité version 2.0 fournit une méthodologie complète, comparative et fondée sur l'expérience pour évaluer l'engagement et la maturité des pays à combler la brèche entre leur niveau actuelle en matière de cybersécurité et les capacités cybernétiques nationales nécessaires pour soutenir le développement à venir du numérique. Cet indice reprend plus de soixante-dix indicateurs uniques autour de sept éléments essentiels pour définir les activités opérationnelles et identifier les domaines à améliorer dans les catégories suivantes : (1) stratégie nationale; (2) réponse aux incidents; (3) cybercriminalité et application de la loi; (4) partage d'informations; (5) investissement dans la Recherche et Développement; (6) la diplomatie commerciale et (7) la défense et réponse aux crises. Le plan d'action qui en résulte fournit une feuille de route à suivre par les pays pour la réduction des risques. Plus important encore, l'Indice de préparation à la lutte contre la cybercriminalité version 2.0 établit un lien entre la croissance économique et l'élaboration de politiques nationales de sécurité. Il reconnaît également que la réalisation du plein potentiel de l'économie Internet en termes de croissance du PIB, de productivité et d'efficacité accrues, d'amélioration des compétences de la main-d'œuvre et d'un meilleur accès aux affaires et à l'information, exige d'aligner les stratégies de développement économique avec les priorités nationales en matière de sécurité. En d'autres termes, les technologies de l'information et de la communication ne peuvent assurer une croissance économique que si les politiques, processus et technologies sont mis en œuvres pour protéger et sécuriser l'infrastructure et les services cybernétiques desquelles dépendent l'avenir numérique et la croissance d'un pays. L'Indice version 2.0 met l'accent sur les outils tels que les politiques, la législation, les réglementations, les normes, les incitations sur le marché et d'autres initiatives que les responsables mondiaux peuvent utiliser afin de protéger leurs investissements numériques et lutter contre l'érosion économique actuelle émanant de la *cyber insécurité*.

Le Modèle de maturité de la capacité de cybersécurité (Capability Maturity Model - CMM) publié, en 2016, par le Centre Mondiale des Capacités de Cybersécurité (GCSCC) de l'Université d'Oxford, détermine les différents niveaux de maturité des pays sur le sujet de la cybersécurité, d'après l'analyse de cinq dimensions : (1) politique et stratégie de cybersécurité; (2) culture et société cybernétique; (3) éducation, formation et compétences en matière de cybersécurité; (4) cadre légal et réglementaire et (5) les normes, organisations et technologies. Chacune de ces dimensions est ensuite décomposée en facteurs et indicateurs plus spécifiques qui, pris ensemble, sont représentatifs d'un niveau plus élevé de maturité en matière de cybersécurité. Le CMM se fonde sur deux méthodes pour déterminer le niveau de préparation à la lutte contre la cybercriminalité. La première méthode utilise un outil d'enquête (semblable à celui de l'UIT) où un état peut lui-même déterminer son niveau de préparation. Ensuite, les réponses au sondage sont examinées puis une équipe participe à un atelier technique d'échange sur la cybercriminalité avec les acteurs clés du secteur gouvernemental, universitaire, privé et public afin de mieux évaluer le niveau de capacité en matière de lutte contre la cybercriminalité à travers cinq niveaux de maturité (initial, formateur, établi, stratégique et dynamique). Le CMM d'Oxford est un excellent outil qui permet de mesurer la compréhension des acteurs clés de l'état actuel des capacités en matière de lutte contre la cybercriminalité et du niveau de maturité du pays. Cela fournit des renseignements nécessaires pour les futurs objectifs politiques et de réduction des risques.

Finalement, en mai 2016, l'Académie de la gouvernance électronique de l'Estonie a publié un indice national de cybersécurité (NCSI), lors de la conférence de Tallinn sur la gouvernance électronique, et a mis à jour/modifié la méthodologie. Une nouvelle version sortira en janvier 2018.[20] La méthodologie incorpore les leçons tirées par l'Estonie. En effet, ce pays fut l'un des premiers à opter pour la gouvernance électronique de la société dans son ensemble. L'indice national de cybersécurité (NCSI) version 2.0 comprend douze domaines de compétences et 46 indicateurs permettant d'évaluer la capacité d'un pays, au niveau national, à construire un état électronique « sécurisé » qui garantit la sécurité des données et transactions tout en limitant l'exposition aux risques numériques. Ces douze domaines d'évaluation des capacités sont les suivants : (1) Capacité à élaborer des politiques nationales de cybersécurité; (2) Capacité à analyser les cybermenaces au niveau national; (3) Capacité à assurer une éducation en matière de cybersécurité; (4) Capacité à garantir une cybersécurité de base; (5) Capacité à assurer un environnement sécurisé pour les services électroniques; (6) Capacité à fournir une infrastructure pour l'identification électronique et les signatures électronique; (7) Capacité à garantir la protection de l'infrastructure d'informations critiques; (8) Capacité à détecter et répondre aux incidents cybernétiques 24 heures sur 24, 7 jours sur 7; (9) Capacité à gérer une crise cybernétique à grande échelle; (10) Capacité à lutter contre la cybercriminalité; (11) Capacité à mener des opérations militaires de cyberdéfense et (12) Capacité à garantir une cybersécurité internationale. L'indice national de cybersécurité prend en compte de nombreux éléments semblables à ceux des autres cadres mais comporte des sections distinctes propres à l'expérience de l'Estonie en matière de gouvernance électronique. Le pays a notamment promu la création d'un environnement sécurisé pour les services électroniques et la fourniture d'identification électronique et de signatures électroniques.

Résumé du cadre

Chaque cadre adopte une approche légèrement différente afin d'aider à renforcer le niveau de cybersécurité d'un pays et à gérer les risques cybernétiques au niveau national. Ces cadres existants ont de nombreux points communs : la reconnaissance du fait que, à l'ère moderne, la sécurité nationale et le bien-être économique des pays dépendent fortement de leur capacité à sécuriser leurs infrastructures cybernétiques nationales et leurs économies numériques; un besoin de promouvoir la cybersécurité aux plus hauts niveaux du gouvernement et auprès des dirigeants d'entreprise; une condition préalable pour débuter la protection des infrastructures les plus critiques et des services essentiels; l'obligation d'élaboration de cadres juridiques et réglementaires appropriés pour protéger la société contre la cybercriminalité, la perturbation des services et la destruction de biens; le besoin pour les secteurs public et privé, ainsi que pour les communautés internationales et régionales, de collaborer ensemble afin d'assurer l'adoption de stratégies efficaces en terme de gestion des risques cybernétiques et de résilience, puis finalement, l'obligation de développer les capacités nationales nécessaires à l'accroissement de la confiance et la sécurité dans l'utilisation des Technologies de l'Information et de la Communication, corriger les lacunes et répondre aux risques importants de cybersécurité.

4

SE PRÉPARER EN MATIÈRE CYBERNÉTIQUE

GÉRER LE RISQUE

Malgré les différents modèles et cadres disponibles permettant aux responsables nationaux de diagnostiquer, évaluer et réduire les risques cybernétiques de leurs pays ainsi que les nombreux appels à l'action des professionnels de l'industrie et des experts en cybersécurité, l'amélioration de la cybersécurité au niveau national continue toutefois de poser problème. Les Pays-Bas ont ainsi reconnu que leur santé économique à venir reposait sur une économie numérique fiable et performante. Ils ont donc consacré des fonds nécessaires et créé un centre pour que le pays puisse atteindre ses objectifs en toute sécurité. En juillet 2015, le Coordonnateur national pour la sécurité et la lutte contre le terrorisme *(National Coordinator for Security and Counterterrorism)* a effectué un « examen de la politique sur les infrastructures critiques ». Dans le cadre de cet examen, le gouvernement a définit l'infrastructure critique comme étant « un ensemble de produits, services et processus sous-jacents nécessaires au fonctionnement du pays [et qui] doivent être sûrs, capables de résister et de se remettre rapidement de tous les dangers. »[21] Toutefois, à partir de l'attaque de NotPetya en 2017 sur le port de Rotterdam (le plus grand port d'Europe) qui engendra des dommages considérables et une dégradation des services, les autorités ont commencé à examiner l'état des systèmes portuaires dépendants d'Internet. Cet examen a mis à jour le fait que l'infrastructure du port n'avait pas été jugée comme critique par leur stratégie nationale de cybersécurité et les politiques de protection des infrastructures.

Dans le même temps, des pays comme le Royaume-Uni, qui avaient identifié des secteurs critiques spécifiques tels que celui de la santé (qui doivent satisfaire à une norme sur les soins de santé), ne tenaient pas compte du fait que les professionnels de la santé ne seraient pas prêts à investir dans la mise à jour de leur logiciel pour protéger ces services critiques contre les risques cybernétiques. Par conséquent, lorsque 81 des 236 services nationaux de santé *(National Health Services)* se sont vus victimes d'un simple ransomware, le WannaCry, un incident qui aurait pu être facilement évité, des vies ont été mises en danger. Le Royaume-Uni a donc été contraint d'examiner son programme de cybersécurité des services critiques afin de voir s'il était suffisant, puis a dû déterminer si une intervention supplémentaire du gouvernement était nécessaire pour gérer le risque.

Comme indiqué précédemment, l'Allemagne et les États-Unis ont identifié les quelques entreprises qui représentent au moins 2% du PIB du leur pays. Ces entreprises sont considérées comme méritant une protection supplémentaire ainsi que davantage de collaboration et échange d'informations de la part du gouvernement. Pourtant, l'échange d'informations entre le gouvernement et l'industrie n'a pas protégé les entreprises des ravages de NotPetya. Bien que les deux pays bénéficient de processus d'échange d'informations et « avertissent » les entreprises de possibles attaques, dans ce cas précis, l'avertissement d'une attaque imminente n'a pas été transmis. Les entreprises de ces deux pays ont donc été fortement touchées et le commerce électronique mondial a dû faire face à des retards de plusieurs semaines voire même de plusieurs mois en raison de leur manque de préparation et de soutien approprié de leurs gouvernements. Finalement, les principales compagnies énergétiques d'Arabie Saoudite qui fournissent près de 25% du gaz naturel liquide et alimentent les systèmes de transport du monde entier, ont été mises hors service en raison d'autres activités cybermalveillantes qui ont eu un impact sur les systèmes de transport et sur l'économie au niveau mondiale.

Tout comme ces exemples le prouvent, aucun pays n'est suffisamment préparer pour lutter contre la cybercriminalité et cette préparation doit débuter par une approche rigoureuse de la gestion des risques. Une gestion efficace des risques exige, avant tout, que les responsables des pays déterminent ce qui compte le plus pour leurs pays, ce qu'il faut protéger à tout prix et qu'ils soient prêt à investir du capital politique, du temps, de l'argent et des ressources nécessaires afin de les protéger.

La Colombie, par exemple, a développé une approche de la gestion des risques permettant d'évaluer son niveau de préparation

à la lutte contre la cybercriminalité et de promouvoir la confiance de la société dans l'utilisation du monde numérique. En effet, les efforts ont abouti à une politique nationale de sécurité numérique colombienne (stratégie nationale de cybersécurité), qui a été approuvée en avril 2016 par le Conseil national de sécurité numérique au travers de la publication du document CONPES 3854 de 2016. La Colombie a adopté les recommandations de l'OCDE sur la gestion des risques et les a utilisées de même que celles de l'OEA, de l'UIT et de l'Organisation du Traité de l'Atlantique Nord (OTAN) afin d'évaluer les menaces numériques pour le pays et comprendre quels étaient les biens critiques menacés.[22] L'étude a poussé le pays à évaluer les principaux risques cybernétiques auxquels il était confronté, à identifier la façon dont les incidents cybernétiques affectent les organisations colombiennes tant du secteur privé que du secteur public, puis à faire de la cybersécurité une priorité et un élément fort de son développement socioéconomique. Cette approche a également aidé à sensibiliser les différentes parties prenantes du pays aux types de menaces, attaques et incidents cybernétiques communs et uniques qui affectent les entités et les entreprises du secteur public et qui se ressentent au niveau économique. La Colombie a reconnu que la gestion des risques cybernétiques au niveau national est une condition sine qua non pour la numérisation des différents secteurs et la transformation numérique du pays.

L'expérience colombienne démontre que la gestion des risques commence par le leadership et la gouvernance. Comme le soulignent la plupart des cadres, des indices et des guides publiés au cours des dernières années par les diverses organisations intergouvernementales, les universitaires et les communautés techniques, il est essentiel d'évaluer ce qui est véritablement vulnérable et placer la cybersécurité au cœur de la stratégie de sécurité nationale. Cependant, il ne suffit pas de faire de la cybersécurité la priorité d'une catégorie autonome et de la traiter comme une question essentiellement nationale. En effet, la cybersécurité est également étroitement liée à la connectivité Internet et à l'adoption rapide des technologies de l'information et de la communication qui, lorsqu'elles sont sûres et résilientes, peuvent favoriser la croissance économique et la prospérité. Par conséquent, il est également important d'aligner les initiatives économiques avec la sécurité, le développement et la résilience (*évaluer la valeur à risque* et élaborer une stratégie nationale qui gère les activités de réduction des risques).

Évaluer le risque

Les responsables nationaux doivent clairement manifester leur volonté de tirer parti de l'environnement numérique ouvert pour une plus grande prospérité économique et sociale en réduisant le niveau global de risques en matière de sécurité numérique aussi bien à l'intérieur qu'à l'extérieur des frontières. Ils doivent être conscient du fait que les risques peuvent changer avec le temps en fonction des mesures prises par au moins deux acteurs : l'attaquant, qui obtient et utilise les compétences permettant de causer des dommages puis, la cible visée, qui peut prendre des précautions pour résister ou contrecarrer le danger duquel elle est victime. Les responsables nationaux doivent s'engager à réduire les risques et accroître la résilience en réalisant des évaluations permanentes des risques tant au niveau national que par secteurs et en adoptant des mesures, des politiques et des processus appropriés pour gérer les risques identifiés.

Afin d'atteindre ces objectifs primordiaux, les responsables nationaux, les décideurs politiques et les autres acteurs de chaque pays doivent travailler ensemble à l'évaluation du risque. La planification stratégique et la réflexion peuvent aider à déterminer le niveau de préparation :

- Quelle est la stratégie à court et à long terme pour le pays ? Quels sont les politiques industrielles, les objectifs économiques et les priorités de sécurité au niveau national ?

- Qu'est-ce qui pourrait mettre en péril ces objectifs? En d'autres termes, quelles faiblesses pourraient être exploitées (des actifs de grande valeur non comptabilisés) et pourraient perturber l'exécution de ces objectifs ?

- Existe-t-il une chaîne de responsabilité claire permettant d'assurer la mise en œuvre des objectifs du pays ? Est-ce que des mesures de réduction des risques ont été mises en place ?

- La cybersécurité et la résilience ont-elles été placées au cœur du processus de planification ?

Cette évaluation étayée et complète mettra en évidence les domaines critiques les plus dépendants à l'égard du numérique (par exemple : les entreprises, les services, les infrastructures et les actifs) qui, si touchés, provoqueront de graves conséquences économiques et sécuritaires pour le pays. Une fois les éléments vulnérables identifiés, ceux qui pourraient mettre en péril les « joyaux de la couronne » du pays et après avoir analysé la probabilité qu'ils soient exposés à tout danger, dommage ou perte, les décideurs pourront-ils prendre des mesures correctives pour contrecarrer ou mitiger ces risques ?

5 RÉDUIRE LES RISQUES AU TRAVERS D'UNE PLANIFICATION MINUTIEUSE

Un pays pourra élaborer un plan de réduction des risques pour combler l'écart entre son niveau actuel de cybersécurité et les compétences cybernétiques nécessaires, au niveau national, pour corriger les lacunes et soutenir les futures priorités économiques et sécuritaires du pays, après la réalisation d'une évaluation des risques. Les efforts de réduction des risques doivent être dirigés par une autorité nationale compétente en matière de cybersécurité. Il s'agira d'un responsable (à la fois une personne et une entité) positionné au plus haut niveau du gouvernement qui puisse orienter, coordonner les actions, surveiller la mise en œuvre du plan, rende des comptes à l'égard de toute faille et qui soit responsable de tout résultat obtenu. Étant donné que la cybersécurité est un sujet transversal à d'autres domaines (droits de l'homme, développement économique, commerce, contrôle des armes, technologies à double usage, sécurité, stabilité, paix et résolution des conflits), il est important de veiller à ce que l'entité nationale compétente en la matière dispose de l'autorité, la responsabilité et le pouvoir suffisant permettant d'impliquer et orienter autant d'acteurs que nécessaire.

Bien qu'il existe un large éventail d'éléments pour la réduction des risques comme le démontrent les différents cadres exposés dans les sections précédentes, les responsables nationaux devraient s'efforcer de comprendre le panorama des risques cybernétiques et menaces spécifiques à leurs infrastructures en réseau. Ces menaces devraient être clairement décrites dans leurs stratégies nationales de cybersécurité et dans l'évaluation nationale des risques cybernétiques. Ils devraient également travailler avec tous les acteurs concernés pour mieux planifier leurs défenses et mieux allouer les ressources humaines et financières nécessaires à la réduction de ces risques. Une planification stratégique et un dialogue peuvent aider à déterminer l'état de préparation d'un pays :

- Communiquer sur ce qui est en jeu et encourager la prise de conscience des risques à tous les niveaux, des responsables gouvernementaux aux citoyens. Les gens ne peuvent valoriser la sécurité sans comprendre auparavant que leurs activités quotidiennes sont menacées (et pas seulement leurs informations personnelles). Par conséquent, le gouvernement devrait lancer une campagne nationale de sensibilisation, promouvoir l'éducation, la formation, le développement des compétences et donner la possibilité aux citoyens de faire partie de la solution à travers la construction d'une culture plus solide en matière de cybersécurité.

- Identifier, hiérarchiser et concentrer les ressources nécessaires sur les actifs de grande valeur et les systèmes critiques qui nécessitent des niveaux de protection accrus. Il s'agit des domaines les plus dépendant du numérique dans le pays (entreprises, infrastructures, services et actifs). Puis, en comprendre les vulnérabilités et hiérarchiser les mesures de sécurité appropriées de façon proportionnelle au risque économique et sociétal.

- Élaborer des cadres juridiques et réglementaires appropriés pour protéger la société contre la cybercriminalité, la perturbation des services et la destruction des biens.

- Utiliser un large éventail d'outils tels que les politiques, la législation, les réglementations, les normes, les incitations sur le marché, les mécanismes volontaires d'application de la loi et autres initiatives pour accroître la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication et corriger les lacunes des processus et des produits (exemples: Directive NIS, Loi chinoise sur la cybersécurité, cadre NIST).

• Améliorer la compréhension de la situation, les indicateurs de menace et les avertissements en surveillant constamment les menaces qui pèsent sur la société en réseau et en utilisant les dernières technologies pour détecter, repousser et contenir ces menaces.

• Développer les compétences nationales nécessaires pour accroître la préparation, la planification de la poursuite des activités et la réponse aux risques importants en matière de cybersécurité lorsque ceux-ci surviennent (cybercrise à grande échelle).

• Engager la communauté internationale à améliorer la sécurité, fiabilité et résilience mondiale des réseaux interopérables (réseaux financiers, des télécommunications, de l'énergie, etc...) à travers la mise en œuvre de normes de sécurité mondiales et la promotion d'accords multilatéraux.

• Anticiper les progrès technologiques futurs, évaluer les nouvelles vulnérabilités pour le pays et la façon dont celles-ci pourraient s'avérer être des opportunités permettant de renforcer la sécurité, la fiabilité et la résilience des infrastructures et actifs de nouvelle génération.

La mise en œuvre efficace de ces tâches et d'autres activités exigera que les rôles, les responsabilités, les processus, les droits de décision et les mécanismes de responsabilisation soient clairement définis. La mise en place d'objectifs de rendement des différents services ministériels ou gouvernementaux et des institutions ou individus responsables de tâches spécifiques au sein du plan d'action, permettra de meilleurs résultats.

Bien évidemment, les activités de réduction des risques nécessitent également l'allocation de ressources dédiées et appropriées pour leur mise en œuvre. Les sources et mécanismes de financement inefficaces peuvent compromettre les résultats escomptés et diminuer la responsabilité des entités chargées de la cybersécurité de la nation qui ne disposent pas de ressources nécessaires pour mener à bien leurs missions. Les ressources devraient être définies en termes d'argent (budget dédié), de personnel, de matériel ainsi que de relations et partenariats nécessaires à une exécution réussi des plans d'atténuation des risques. Dans le cadre d'une stratégie nationale de cybersécurité, l'attribution de ressources pour atteindre les objectifs et mener à bien les tâches ne doit pas être considérée comme une initiative ponctuelle. Un financement suffisant, cohérent et continu est à la base d'un niveau efficace de lutte contre la cybercriminalité. Les ressources peuvent être allouées par tâche, par objectif ou par entité gouvernementale. Le gouvernement pourra également envisager l'établissement d'un budget central pour la cybersécurité, géré par un mécanisme central de gouvernance de la cybersécurité. Qu'il s'agisse de regrouper diverses sources de financement en un programme cohérent et intégré ou de créer un budget unifié inter-gouvernementale, le programme global devra avoir des étapes et des échéances clairement définies afin d'assurer la mise en œuvre réussie de la stratégie.

Évaluation permanente du risque

Lorsque les efforts de cybersécurité se transforment en une évaluation ponctuelle (cadre de conformité), plutôt qu'en une évaluation permanente du risque, ils échouent. La gestion des risques nécessite une anticipation proactive des menaces et une évaluation continuelle des vulnérabilités au sein des domaines critiques les plus dépendants du numériques (les entreprises, les infrastructures, les services et les actifs). Comme indiqué ci-dessus, il existe un certain nombre de cadres qui soulignent l'importance d'une évaluation continue des risques et de la correction des défaillances de contrôle. Les pays devraient inclure dans leurs architectures nationales de cybersécurité des mécanismes de suivi et de mesure de la performance et l'exécution des initiatives en matière de cybersécurité (activités de réduction des risques). Une évaluation continue du plan de mise en œuvre (c'est-à-dire de ce qui va bien et ce qui ne va pas) permet de réaliser des ajustements et de promouvoir davantage la stratégie globale. Les mécanismes de bonne gouvernance fixent les responsabilités permettant d'assurer une bonne exécution. De plus, les paramètres ou indicateurs clés de performance (KPI), exploitables, reproductibles, significatifs et datés doivent être utilisés pour renforcer les objectifs et échéances réalistes. Les indicateurs de performance ou paramètres clés doivent répondre aux critères suivants :

• ***Spécifique :*** cibler un domaine spécifique à améliorer.

• ***Mesurable :*** quantifier, ou tout du moins, suggérer un indicateur de progrès.

• ***Réalisable :*** indiquer les résultats pouvant être réellement atteints, compte tenu des ressources disponibles.

• ***Actionnable :*** il y a des actions claires à mettre en œuvre.

• ***Responsable :*** préciser qui le fera.

• ***Temps :*** indiquer quand est-ce que le(s) résultat(s) pourra (pourront) être atteint(s).

Bien qu'aucun pays ne soit entièrement prêt en matière de cyberdéfense et que les risques cybernétiques ne peuvent être entièrement éliminés, ils peuvent et doivent cependant être gérés. La préparation à la lutte contre la cybercriminalité commence par une approche efficace de la gestion des risques qui comprend une vision claire des actifs de grande valeur du pays et des systèmes critiques qui nécessitent des niveaux de protection accrus. Il s'agit des domaines les plus dépendant du numérique du pays (entreprises, infrastructures, services et actifs). Une fois ceux-ci identifiés, une analyse des risques et une évaluation des vulnérabilités peuvent définir et hiérarchiser les mesures de sécurité nécessaires pour corriger les lacunes. Ces mesures seront appropriées et proportionnelles au risque économique et sociétal.

Ce n'est que par le biais d'efforts concertés et coordonnés entre les parties prenantes, au niveau national, qu'il sera possible de réduire de manière significative les risques cybernétiques et d'aller de l'avant pour assurer la sûreté et la sécurité futures du pays.

5

CONCLUSION

La *cyber insécurité* grandit. Le volume, la portée, l'ampleur et la sophistication des cybermenaces contre les services et les infrastructures critiques des pays, dépassent les mesures de défense. Les activités cybernétiques actuelles, destructrices et déstabilisantes, exigent des gouvernements qu'ils prennent des mesures urgentes et investissent pour faire passer leurs pays d'un état de cyber-insécurité à un niveau adéquat de préparation à la lutte contre la cybercriminalité. Les pertes s'accumulent, le mal augmente et le danger est imminent.

Les responsables nationaux doivent élaborer des stratégies nationales de cybersécurité qui envisagent une autorité dédiée et compétente qui soit responsable du niveau de cybersécurité du pays. Une compréhension des risques encourus doit être réalisée à tous les niveaux, depuis les responsables gouvernementaux jusqu'aux citoyens. Tous devraient pouvoir comprendre les vulnérabilités de l'environnement numérique du pays et connaître leur rôle dans l'atténuation des risques. Cette feuille de route stratégique permet l'adoption de mesures, politiques et processus appropriés pour corriger les lacunes et réduire les risques pour la société, l'économie et le pays. Ceci ne peut se faire sans ressources dédiées au financement des initiatives pour la réduction des risques et l'accroissement de la résilience. L'adoption d'une stratégie nationale en matière de cybersécurité est une étape primordiale dans la sécurisation de l'infrastructure et des services cybernétiques nationaux desquels dépendent le futur numérique et le bien-être économique d'une nation moderne.

6

À PROPOS DE L'AUTEUR

Melissa Hathaway est une grande spécialiste des questions de politique liées au cyberespace et à la cybersécurité. Elle a servi dans deux administrations présidentielles où elle fut à l'origine de l'examen de la politique relative au cyberespace qui a été réalisé pour le président Barack Obama, et où elle a eu l'occasion de diriger le projet global sur la cybersécurité nationale pour le président George W. Bush. En tant que présidente de Hathaway Global Strategies LLC, elle conseille les secteurs public et privé et apporte un regard unique mêlant expertise politique et technique à une expérience au sein de conseil d'administrations qui permet de mieux comprendre l'articulation existant entre les politiques gouvernementales, les tendances technologiques et industrielles montantes et les facteurs économiques ayant une incidence sur les stratégies d'acquisitions et de développement des affaires dans ce domaine. Elle a élaboré une méthodologie unique de mesure et d'évaluation des niveaux de préparation à la lutte contre certains risques liés à la cybersécurité, mieux connue sous le nom « d'Indice de préparation à la lutte contre la cybercriminalité » (Cyber Readiness Index). Vous pourrez trouver plus d'informations sur l'Indice de préparation à la lutte contre la cybercriminalité version 2.0 sur : **www.potomcinstitute.org/academic-centers/cyber-readiness-index.**

Melissa Hathaway publie régulièrement des articles sur des thèmes liés à la cybersécurité qui touchent les pays et les entreprises. La plupart de ses articles peuvent être consultés sur les sites internet suivants :
www.belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html et
www.ctm.columbia.edu/people/melissa-hathaway

5 RÉFÉRENCES

1. Dictionnaire d'Oxford. Le SP 800-30 du NIST (Rév. A) définit le risque de la façon suivante : Risque = Menace x Vulnérabilité. Selon la GRC, les énoncés de risque se définissent de la façon suivante : Risque = Condition (Probabilité) + Conséquence (Impact).

2. Nicolas Rapp et Robert Hackett, "A Hackers Toolkit". Fortune Magazine 25 octobre 2017, https://fortune.com/2017/10/25/cybercrime-spyware-marketplace/

3. Eduard Kovaks, "Shadow Brokers Want $20,000 for Weekly Leaks," Security Magazine, 30 mai 2017, https://www.securityweek.com/shadow-brokers-want-20000-monthly-leaks; et
Eduard Kovaks, "Shadow Brokers Promise More Exploits for Monthly Fee," Security Magazine, 16 mai 2017, https://www.securityweek.com/shadow-brokers-promise-more-exploits-monthly-fee; et
Nicole Perloth, "A Cyberattack the 'World Isn't Ready For,'" The New York Times, 22 juin 2017, https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html?_r=0

4. National Audit Office, "Investigation: WannaCry cyber attack and the NHS," 27 octobre 2017, https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

5. Richard Chirgwin, "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz," The Register, 25 janvier 2018, https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/.

6. NotPetya a perturbé les activités et détruit un grand nombre d'immobilisations à l'échelle mondiale. Rapports publiés par AP Moller-Maersk, Balersdorf, DHL, DLA Piper, Federal Express, Merck, Mondolez, Nuance, le groupe Reckitt Benckiser, Rosnett, Saint Gobain et WPP qui affichent des pertes d'au moins 2,5 milliards de dollars. Un rapport récent de la Lloyds de Londres tire la sonnette d'alarme et explique qu'une cyberattaque réussi au niveau mondial, pourrait provoquer des dommages pour un montant compris entre 53,1 et 121,4 milliards de dollars. Voir : Lloyds of London, "Extreme Cyber-Attack Could Cost as Much as Superstorm Sandy," 17 juillet 2017, https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report.

7. Kelly Jackson Higgins, "Schneider Electric: TRITON / TRISIS ttack Used 0-Day Flaw in its Safety Controller System, and a RAT," Dark Reading, 18 janvier 2018, https://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.

8. Les domaines de premier niveau (par exemple, .mil, .com, .edu, .gov) ont été introduits en 1985 et ont permis d'établir un cadre pour le commerce électronique mondial. L'innovation a continué d'introduire de nouvelles technologies. En effet, la création du langage de balisage hypertexte (HTML) en 1990 a permis un partage plus important d'informations facilement compréhensibles sur Internet et a finalement donné naissance à la toile (World Wide Web). D'autres avancées technologiques ont également vu le jour : les messages textes (SMS) (1992), la Voix sur IP (1996), le WiFi (1997), wikipedia (2001), le moteur de recherche Google (1997), les réseaux sociaux (2002) et la voix et vidéo sur IP avec Skype (2003). Le secteur privé encourage l'innovation et l'adoption de la technologie en promettant la réduction des coûts, l'augmentation de la productivité et son utilisation massive par les consommateurs sans insister sur les questions de sécurité. Voir : Melissa Hathaway, "Falling Prey to Cybercrime: Implications for Business and the Economy,", dans la Sécurisation du cyberespace : un nouveau domaine pour la sécurité nationale, février 2012, Aspen Institute Press.

9. Nombre de pays sont ceux qui ont une définition différente des infrastructures critiques. Pour les besoins de ce rapport, nous avons opté pour une définition générale. Voir : Bibliothèque numérique du Département de Sécurité Intérieure, « Presidential Decision Directive 63, PDD / NSC-63 », 22 mai 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm.

10. Les responsables n'ont pas encore défini le nombre de secteurs auxquels s'appliquera la loi. Toutefois, de nombreux experts estiment que cette loi inclura les mêmes secteurs que ceux de la directive européenne sur la sécurité des réseaux et des systèmes d'information (soit ceux de l'énergie, des transports, des banques, des infrastructures des marchés financiers, des infrastructures numériques, de la santé et de l'eau). Voir : Yanqing Hong, "The Cross-border Data Flows Security Assessment: An Important Part of Protecting China's Basic Strategic Resources," 20 juin 2017, Yale Law School, Centre de la Chine, document de travail de Paul Tsai, https://law.yale.edu/system/files/area/center/china/document/dataflowssecurity_final.pdf.

11. NIST, "Cybersecurity 'Rosetta Stone' Celebrates Two Years of Success," 18 février 2016, https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success.

12. Hathaway Global Strategies LLC. Perceptions en matière d'engagement du conseil d'administration et de la direction des sociétés touchées.

13. NIST, "NIST Special Publication 800-37 (Rev. 2) DRAFT — Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy (Discussion Draft)," septembre 2017, https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf.

14. SMSI, Genève 2003 - Tunis 2005, "Tunis Commitment", 18 novembre 2005, http://www.itu.int/net/wsis/docs2/tunis/off/7.html.

15. ITU (2014), Global Cybersecurity Index, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

16. OCDE (2015), Gestion du risque de sécurité numérique pour la prospérité économique et sociale : Recommandation de l'OCDE et Document d'accompagnement, Éditions OCDE, Paris https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

17. WEF (2018), Cyber Resilience Playbook for Public-Private Collaboration, pp. 33-36, https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration.

18. Ibid.

19. Cet indice s'appuie sur l'Indice précédent, la version 1.0, qui fournissait un cadre méthodologique permettant d'évaluer la préparation à la lutte contre la cybercriminalité au travers de cinq éléments essentiels : la stratégie nationale en matière de cybercriminalité, la réponse aux incidents, la cybercriminalité et la capacité juridique, le partage d'informations et la recherche et développement en matière de cybercriminalité. L'Indice de préparation à la lutte contre la cybercriminalité version 1.0 a appliqué cette méthodologie à un groupe initial de trente-cinq pays. Pour plus d'informations sur Indice de préparation à la lutte contre la cybercriminalité version 1.0, voir : Melissa Hathaway, "Cyber Readiness Index 1.0," Hathaway Global Strategies LLC (2013), http:// belfercenter.ksg.harvard.edu/ les/ cyber-readiness-index-1point0.pdf.

20. NCSI, "NCSI Methodology" http://ncsi.ega.ee/methodology (1.0) et http://ncsi.ega.ee/ncsi-methodology-2-0-launched/ (2.0).

21. Coordonnateur national pour la sécurité et la lutte contre le terrorisme, "Review of Policy on Critical Infrastructure," juillet 2015. Melissa Hathaway et Francesca Spidalieri, "The Netherlands Cyber Readiness at a Glance," mai 2017, Institut d'études politiques du Potomac, http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf.

22. OEA, MINTIC, BID (2017), Impact des incidents de sécurité numérique en Colombie 2017, https://publications.iadb.org/handle/11319/8552.

OEA
Plus de droits
pour plus de personnes

GÉRER LE RISQUE CYBERNÉTIQUE
— AU NIVEAU NATIONAL —

White paper series
Édition 2

2018