INDICE DE PRÉPARATION À LA LUTTE CONTRE LA CYBER-CRIMINALITÉ – VERSION 2.0

PROGRAMME DE PRÉPARATION À LA LUTTE CONTRE LA CYBERCRIMINALITÉ : ÉTUDE DE RÉFÉRENCE ET INDICE

Auteure principale : Melissa Hathaway

Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri

Novembre 2015

POTOMAC INSTITUTE FOR POLICY STUDIES

Copyright © 2015, Indice de préparation à la lutte contre la cybercriminalité, Tous droits réservés.

Publié par le Potomac Institute for Policy Studies (Potomac)

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA, 22203
www.potomacinstitute.org
Téléphone : +1 703.525.0770; Fax : +1 703.525.0299

E-mail: *CyberReadinessIndex2.0@potomacinstitute.org*

Suivez-nous sur Twitter :
@CyberReadyIndex

Remerciements

Le Potomac Institute for Policy Studies souhaite remercier les Applications TIC et la division de la cybersécurité de l'Union internationale des télécommunications (UIT) ainsi que le Comité interaméricain de lutte contre le terrorisme de l'Organisation des États américains pour leur soutien permanent. Les auteurs souhaitent également remercier Sherry Loveless et Alex Taliesen pour leur travail de conception et d'édition.

INDICE DE PRÉPARATION À LA LUTTE CONTRE LA CYBER-CRIMINALITÉ – VERSION 2.0

PROGRAMME DE PRÉPARATION À LA LUTTE CONTRE LA CYBERCRIMINALITÉ : ÉTUDE DE RÉFÉRENCE ET INDICE

TABLE DES MATIÈRES

INTRODUCTION 1

CONTEXTE 2

INDICE DE PRÉPARATION À LA LUTTE CONTRE LA CYBERCRIMINALITÉ (VERSION 2.0) — MÉTHODOLOGIE . . 3

1. STRATÉGIE NATIONALE 6

2. RÉPONSE AUX INCIDENTS. 9

3. CYBERCRIMINALITÉ ET APPLICATION DES LOIS 13

4. PARTAGE DES INFORMATIONS 17

5. INVESTISSEMENT DANS LA RECHERCHE ET LE DÉVELOPPEMENT . . 20

6. DIPLOMATIE COMMERCIALE 24

7. DÉFENSE ET RÉPONSE AUX CRISES 28

CONCLUSION 31

BIBLIOGRAPHIE 33

À PROPOS DES AUTEURS. 43

INDICE DE PRÉPARATION À LA LUTTE CONTRE LA CYBER-CRIMINALITÉ – VERSION 2.0

PROGRAMME DE PRÉPARATION À LA LUTTE CONTRE LA CYBERCRIMINALITÉ : ÉTUDE DE RÉFÉRENCE ET INDICE

Auteure principale : Melissa Hathaway
Chris Demchak, Jason Kerben,
Jennifer McArdle, Francesca Spidalieri

La version 2.0 « Indice de préparation à la lutte contre la cybercriminalité » est une version étendue de la version 1.0 « Indice de préparation à la lutte contre la cybercriminalité », publiée en novembre 2013.

INTRODUCTION

Actuellement, aucun pays n'est capable de lutter contre la cybercriminalité.

Il est évident que la croissance économique mondiale dépend de plus en plus de l'adoption rapide des technologies de l'information et de la communication (TIC), et de la connexion de la société à Internet. En effet, la stratégie numérique de chaque pays promet de stimuler la croissance économique, d'augmenter l'efficacité, d'améliorer les prestations et les capacités de service, de favoriser l'innovation et les gains de productivité, et d'encourager une bonne gouvernance. Et pourtant la disponibilité, l'intégrité et la résistance de cette infrastructure clé sont mises en péril. La quantité, l'étendue, la vélocité et le niveau de complexité des menaces auxquelles sont confrontés nos systèmes et nos infrastructures en réseau sont autant d'éléments bien réels et qui ne cessent de croître. Les violations de données, les activités criminelles, les interruptions de service et la destruction de biens deviennent fréquentes et menacent l'économie de l'Internet.

Les leaders mondiaux reconnaissent qu'une meilleure connectivité Internet favorise la croissance économique uniquement lorsque l'infrastructure sous-jacente et les appareils qui y sont connectés sont protégés et sécurisés. Les pays doivent par conséquent assurer l'harmonisation de leurs visions économiques nationales et de leurs priorités nationales en matière de sécurité.

Il n'existe cependant actuellement toujours aucune méthodologie complète, comparative et empirique permettant d'évaluer l'engagement et la capacité d'un pays à protéger ses infrastructures et ses services numériques nationaux dont dépendent son avenir et sa croissance numériques. L'indice de préparation à la lutte contre la cybercriminalité – Version 1.0 (IPC)[1] présentait une nouvelle manière d'examiner le problème et a été élaboré dans le but de susciter des discussions internationales et d'encourager des actions mondiales pour lutter contre l'érosion économique provoquée par la *cyberinsécurité*.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

Se basant sur l'IPC 1.0, le document intitulé « Indice de préparation à la lutte contre la cybercriminalité – Version 2.0 » étudie cent vingt cinq pays ayant adopté ou adoptant actuellement les TIC et l'Internet. À cet effet il applique une méthodologie objective pour évaluer, à l'aide de sept éléments essentiels, l'engagement et la capacité de chaque pays en matière de cybersécurité. En appliquant cette méthodologie, un pays peut mieux comprendre son implication dans le cadre des infrastructures Internet ainsi que les dépendances et les vulnérabilités qui en découlent.[2] De manière plus spécifique, l'IPC 2.0 mesure le niveau de préparation des pays face à certains cyber-risques et il identifie les domaines dans lesquels les leaders nationaux peuvent modifier ou améliorer la position actuelle de leur pays en exploitant ou en changeant les lois, les politiques, les normes, les effets de levier sur les marchés (ex : les primes et réglementations), et en mettant en œuvre d'autres initiatives pour préserver la sécurité de leur connectivité et protéger la valeur de leur économie.

CONTEXTE

La plupart des pays ont adopté des stratégies économiques basées sur les TIC et s'efforcent de fournir aux particuliers et aux entreprises des moyens de communication rapides, efficaces et abordables leur permettant de faire entrer leur société de l'information dans l'ère numérique.[3] Les projets de modernisation tels que le cybergouvernement, la banque en ligne, la cybersanté, l'apprentissage en ligne, les réseaux électriques de nouvelle génération et l'automatisation des différents éléments des infrastructures de transport et d'autres services clés, figurent en tête des priorités économiques de la plupart des pays. Par exemple, l'initiative stratégique « Internet Plus » déployée en Chine a pour but de contribuer activement au développement sain du commerce électronique, des réseaux industriels et de la banque en ligne, mais aussi de favoriser la croissance des nouvelles industries et l'expansion à l'échelle internationale de la zone de couverture Internet des entreprises chinoises.[4] Comme beaucoup d'autres pays, la Chine considère Internet comme l'un des éléments clés de sa croissance et de ses opportunités de développement futurs. De la même manière, le premier ministre indien Narendra Modi a présenté sa vision qui consiste à transformer son pays en une « économie de la connaissance basée sur les technologies numériques », en exploitant les compétences indiennes mondialement renommées en matière de technologie de l'information pour créer des emplois dans les secteurs des télécommunications et informatiques, ainsi que sur les marchés des appareils électroniques. Par ailleurs, l'Inde souhaite innover dans les solutions TIC liées aux domaines de la santé, de la gestion des connaissances et des marchés financiers.[5] Enfin, la Commission européenne tente de créer un important marché unique dédié aux services numériques qui pourra permettre la libre circulation des marchandises, des services, des capitaux et des entreprises. Il est prévu que la mise en œuvre réussie de cette « stratégie de marché unique numérique » engendre en Europe une croissance du PIB supplémentaire estimée à 415 milliards d'euros par an.[6]

Les pays doivent assurer l'harmonisation de leurs visions économiques nationales et de leurs priorités nationales en matière de sécurité.

Les gouvernements, en particulier ceux des pays en voie de développement, font pression pour mettre en œuvre des stratégies d'adoption des TIC encore plus agressives pour offrir des services supplémentaires à plusieurs millions de citoyens dans le but d'élargir et d'accélérer les progrès économiques.[7] De fait, la Banque mondiale estime que pour une tranche de 10 % de la population reliée à Internet, le PIB augmente de 1 à 2 %.[8] En outre, selon une étude récente, les gouvernements et les

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

entreprises prennent toujours plus conscience du fait que l'adoption d'Internet et des TIC permettra d'augmenter durablement leur compétitivité et le bien-être de la société, représentant éventuellement jusqu'à 8 % du PIB national.[9] Certains rapports vont encore plus loin en affirmant que la modernisation des systèmes industriels (ex : les réseaux électriques, les oléoducs et gazoducs, les usines de fabrication, etc.) représente 46 % de l'économie mondiale, un chiffre qui pourrait passer à 50 % au cours des dix prochaines années.[10]

Les nations ne peuvent pas se permettre d'ignorer ce débouché économique. Mais peu d'entre elles prennent en compte l'impact et les coûts économiques associés à des services clés peu fiables, aux expositions/violations de la vie privée des citoyens, au vol de données brevetées d'entreprises et de secrets d'état, ni même l'impact de la cyberfraude et de la cybercriminalité, autant d'éléments qui mènent à une situation sécuritaire instable sur les plans économique et national. En d'autres termes, la cyberinsécurité représente un impôt sur la croissance.[11]

Il est par exemple estimé que le Groupe des Vingt (G20) a perdu 2,5 millions d'emplois en raison de contrefaçons et de piratage, et que, à cause de la cybercriminalité, les gouvernements et les consommateurs perdent chaque année jusqu'à 125 milliards de dollars, incluant notamment des pertes de recettes fiscales.[12] Les États-Unis estiment à 300 milliards de dollars l'impact annuel du vol international de propriété intellectuelle (PI) sur leur économie. Cela représente 1 % de son PIB.[13] D'autres études réalisées aux Pays-Bas, au Royaume-Uni et en Allemagne ont identifié des pertes similaires sur le PIB de ces pays. Aucun pays ne peut se permettre de perdre ne serait-ce qu'1 % de son PIB en raison de cyberactivités illégales. Mais étant donné que les pays continuent d'adopter les TIC et la connectivité Internet, l'exposition, les risques et les coûts économiques vont augmenter de façon exponentielle si la sécurité et la résilience des infrastructures ne sont pas au cœur de leurs stratégies de modernisation.

La cyber-insécurité représente un impôt sur la croissance

Les sociétés connectées résilientes doivent encourager la modernisation en plaçant la sécurité au cœur de leurs priorités.

La prise de conscience de ces pertes pour l'économie forcera les leaders nationaux à mieux harmoniser le programme sécuritaire de leur pays et leur programme économique, et à investir dans la valeur dérivée de ces deux plans.[14] Identifier les pertes économiques résultant de la cyberinsécurité pourra susciter un intérêt national et mondial pour lutter contre cette érosion économique. L'IPC 2.0 sert de cadre aux pays pour qu'ils puissent maintenir, en toute sécurité, la croissance économique d'une société résiliente connectée et basée sur les TIC.

INDICE DE PRÉPARATION À LA LUTTE CONTRE LA CYBER-CRIMINALITÉ (VERSION 2.0) — MÉTHODOLOGIE

L'IPC 2.0 possède deux composantes principales : présenter en premier lieu, aux leaders nationaux les étapes à suivre pour protéger leurs pays de plus en plus connectés ainsi que la croissance potentielle de leur PIB en évaluant de manière objective l'engagement et la capacité de leur pays à lutter contre la cybercriminalité et à faire preuve de résilience. En second lieu, l'IPC explique ce qu'être « prêt à lutter contre la cybercriminalité » signifie pour un pays, et il décrit les éléments clés de l'aptitude à lutter contre la cybercriminalité dans un plan d'action destiné aux différents pays. La méthodologie de l'IPC 2.0 représente un outil convi-

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

vial, unique et utile qui permet d'évaluer l'écart entre l'état actuel d'un pays en matière de cybersécurité et ses cybercapacités nationales pour pouvoir réaliser sa vision économique. Le modèle élaboré et utilisé dans le cadre de cette analyse inclut plus de soixante-dix indicateurs uniques répartis sur sept rubriques :

1. Stratégie nationale ;
2. Réponse aux incidents ;
3. Cybercriminalité et application des lois ;
4. Partage des informations ;
5. Investissement dans la recherche et le développement (R&D) ;
6. Diplomatie commerciale ; et
7. Défense et réponse aux crises.

Pour chaque pays, les évaluations factuelles exploitent des sources primaires, et chaque donnée unique repose sur des recherches empiriques et de la documentation. Les pays font l'objet d'une évaluation pour chaque indicateur et sur trois niveaux d'aptitude à lutter contre la cybercriminalité : éléments de preuve insuffisants, partiellement opérationnel ou entièrement opérationnel.

La méthodologie de l'IPC 2.0 a permis d'évaluer l'aptitude de cent vingt-cinq pays à lutter contre la cybercriminalité en analysant leur engagement et leur capacité à se défendre contre la cybercriminalité et à mettre en place des services et des infrastructures fiables (Figure 1 et tableau 1).

Les pays sélectionnés incluent les soixante-cinq premiers pays figurant dans l'Index sur le développement des TIC (IDT) de l'Union internationale des télécommunications, afin de souligner l'importance de la connexion à Internet et aux TIC. Les membres du G20 ont été inclus car ils représentent 90 % du PIB mondial, 80 % des transactions commerciales internationales, 64 % de la population mondiale et 84 % de l'ensemble des émissions de combustible fossile.

Afin d'effectuer une représentation régionale et mondiale, des pays supplémentaires ont été sélectionnés parmi : l'Organisation de coopération et de développement économique (OCDE), la Communauté économique africaine (CEA), l'Association latino-américaine d'intégration (ALADI), la Coo-

Éléments de preuve insuffisants : Éléments de preuve manquants ou non localisés. Il est toutefois possible que ces données existent mais qu'elles n'aient pas encore été rendues publiques ou classées dans le domaine public.

Partiellement opérationnel : On possède des éléments de preuve sur les politiques, les actions et/ou les opérations de financement mises en place mais ces initiatives sont immatures, incomplètes ou en cours de développement. Bien qu'on ait pu les observer, il est difficile d'évaluer leur fonctionnalité.

Entièrement opérationnel : On possède des éléments de preuve suffisants pour pouvoir évaluer une activité viable et parvenue à maturité.[15]

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

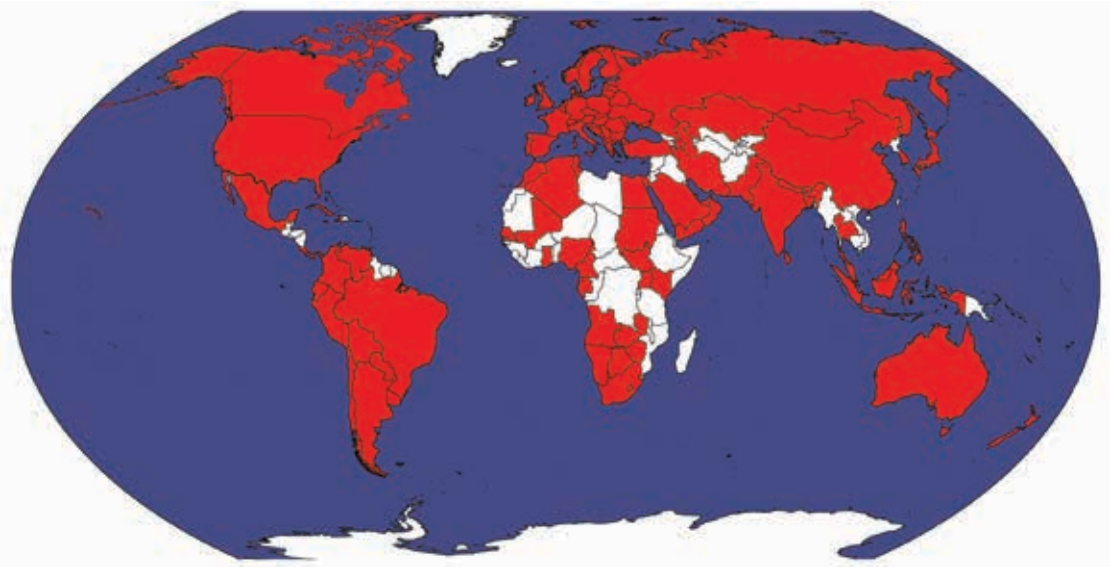

Figure 1 : Pays sélectionnés dans le cadre de l'IPC 2.0

Algérie	Colombie	Israël	Pays-Bas	Sri Lanka
Andorre	Costa Rica	Italie	Nouvelle-Zélande	Saint-Christophe-et-Nevis
Angola	Croatie	Japon	Nigéria	Saint-Vincent et Grenade
Antigua-et-Barbuda	Cuba	Kazakhstan	Norvège	Soudan
Arménie	Chypre	Kenya	Oman	Swaziland
Argentine	République tchèque	République kirghize	Pakistan	Suède
Australie	Danemark	Lettonie	Paraguay	Suisse
Autriche	Djibouti	Liban	Panama	Taïwan
Azerbaïdjan	Équateur	Lesotho	Pérou	Ex-République yougoslave de Macédoine
Bahreïn	Égypte	Lituanie	Philippines	Thaïlande
Bangladesh	Estonie	Luxembourg	Pologne	Trinité-et-Tobago
La Barbade	Finlande	Macao, Chine	Portugal	Tunisie
Biélorussie	France	Malaisie	Qatar	Turquie
Belgique	Gabon	Maldives	Roumanie	Ouganda
Bhoutan	Gambie	Mali	Russie	Ukraine
Bolivie	Allemagne	Malte	Arabie saoudite	Émirats arabes unis
Bosnie-Herzégovine	Ghana	Île Maurice	Sénégal	Royaume-Uni
Botswana	Grèce	Mexique	Serbie	États-Unis d'Amérique
Brésil	Hong Kong	Moldavie	Seychelles	Uruguay
Brunei Darussalam	Hongrie	Mongolie	Singapour	Ouzbékistan
Bulgarie	Islande	Monaco	Slovaquie	Vénézuela
Cameroun	Inde	Monténégro	Slovénie	Vietnam
Canada	Indonésie	Maroc	Afrique du Sud	Yémen
Chili	Iran	Namibie	Corée du Sud	Zambie
Chine	Irlande	Népal	Espagne	Zimbabwe

Tableau 1 : Pays sélectionnés dans le cadre de l'IPC 2.0

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

pération économique de la zone Asie-Pacifique (APEC), la Coopération économique régionale pour l'Asie centrale (CAREC), le Conseil de coopération du Golfe (CCG), l'Association pour la coopération régionale de l'Asie du Sud (SAARC) et la Fédération des commerçants d'Amérique du Nord. Les pays de ces groupes économiques régionaux sont représentés dans l'IDT et sont souvent également inclus dans l'indice de disponibilité de l'Internet du Forum économique mondial (FEM). Cela permet de garantir que les pays sélectionnés adoptent les TIC et investissent dans des services Internet accessibles et abordables pour favoriser la croissance économique

Étant donné que le CCG ne représente pas le Moyen-Orient, trois états parmi les mieux classés en termes de PIB et ne faisant pas partie du CCG ont également été ajoutés : l'Iran, le Yémen et le Liban.[16]

Cet échantillon comprenant cent vingt-cinq pays constitue une part importante de la population mondiale et illustre parfaitement le caractère varié et représentatif des critères de sélection des pays appliqués dans le cadre de l'IPC 2.0.

L'accent que place l'IPC 2.0 sur l'interconnexion entre l'économie et la sécurité (ou le manque de sécurité) fournit à chaque pays une solide base lui permettant d'évaluer son aptitude en matière de cybersécurité. Il constitue également un cadre qui aide à mettre en place des politiques et des stratégies, des initiatives opérationnelles et institutionnelles, des exigences relatives aux ressources, l'élaboration de textes réglementaires et législatifs et divers effets de levier sur les marchés. La mise en œuvre de l'IPC 2.0 fera prendre conscience de la relation qui existe entre un cyberespace durable et la croissance du PIB des pays, étant donné que l'avenir d'un pays sera certainement de plus en plus souvent dominé par les nouvelles technologies et l'utilisation d'Internet. Cette mise en œuvre permet par ailleurs de mieux comprendre le phénomène d'érosion économique créé par la cyberinsécurité et dans quelle mesure les préoccupations liées à la sécurité nationale sont considérées comme faisant partie des priorités numériques et économiques d'un pays. Cette méthodologie peut mener à des décisions analytiques concernant la façon d'anticiper et de répondre à un problème.

Enfin, l'IPC 2.0 fournit aux entités internationales (telles que l'UIT, le FEM, l'Organisation des états américains (OEA), la Banque de développement interaméricaine (BDI), la Banque mondiale et bien d'autres) un cadre et une approche complémentaire à leurs projets respectifs et aux discussions internationales.

Une description détaillée des sept rubriques essentielles incluses dans la méthodologie de l'IPC 2.0 est présentée ci-dessous. Chaque section contient un élément clé et au moins dix indicateurs supplémentaires d'évaluation et qui, une fois combinés, représentent un plan de préparation des pays dans le cadre de la lutte contre la cybercriminalité. En outre, des exemples de pays sont inclus pour illustrer les solutions innovantes et multiculturelles qui peuvent être employées pour se préparer à lutter contre la cybercriminalité. Bien que ces exemples ne soient en aucun cas exhaustifs, ils permettent de mettre en avant des approches spécifiquement conçues pour être adoptées au niveau national.

1. STRATÉGIE NATIONALE

Le premier (et le plus important) élément révélateur du niveau de préparation d'un pays en matière de lutte contre la cybercriminalité est l'élaboration et la publication d'une stratégie nationale de cybersécurité harmonisant parfaitement la vision économique d'un pays et ses priorités nationales en termes de sécurité. L'Internet, les réseaux à haut débit, les applications mobiles, les services informatiques, les logiciels et le matériel informatique constituent les bases de l'économie et de l'avenir numériques d'un pays.[17] L'Internet et les TIC sont devenus le pilier des plateformes familiales (ex : Facebook™, Twitter™, Instagram™, Renren™, VKontakte™, etc.), des moteurs commerciaux, des services et infrastructures critiques et de l'économie mondiale.[18] Les interdépendances et l'hyperconnectivité

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

touchent chaque secteur. Par exemple, les techniques de production avancées emploient des systèmes de contrôle industriels et des technologies robotiques pour augmenter la productivité et réduire le recours aux interventions manuelles. Les activités agricoles modernes intègrent pour les cultures des appareils raccordés à des protocoles Internet (IP ou Internet Protocol) ayant pour fonction de déterminer les besoins en 'engrais et d'ajuster l'approvisionnement en eau. Des appareils IP sont également installés sur le bétail pour identifier les endroits où broutent et boivent les animaux, en évaluant quasiment en permanence l'état de santé de ces derniers. Le commerce électronique, c'est-à-dire la libre circulation des biens et des services entre les pays, modifie le rôle des étalages traditionnels en livrant un ensemble varié d'articles directement chez les acheteurs en ligne après qu'ils ontpassé leur commande sur Internet. Les systèmes de transport utilisent désormais des capteurs, des appareils mobiles et des bornes automatiques pour gérer les activités de circulation et émettre les billets. Les villes connectées utilisent des dispositifs de localisation géographique pour contrôler la vitesse et l'emplacement des véhicules afin de déterminer si un conducteur respecte le code de la route. Dans le secteur des soins de santé, des projets de modernisation numérisent les dossiers médicaux des citoyens et utilisent des installations informatiques basées sur le Cloud pour faciliter l'accès aux dossiers médicaux partout dans le monde. La télémédecine utilise l'Internet haute vitesse pour offrir des conseils et des services médicaux aux zones moins bien desservies. Enfin, les systèmes financiers échangent chaque jour plusieurs milliers de milliards de dollars (les opérations effectuées sur les marchés des matières premières nécessitant l'utilisation de la monnaie numérique) et la banque en ligne élimine toute nécessité de se rendre dans une banque physique locale.

Les menaces auxquelles sont confrontées les infrastructures en réseau ne cessent d'augmenter. Les pays commencent à comprendre ces menaces et évoquent le besoin de protéger les infrastructures et les données, de défendre leur patrie et de recourir à des systèmes de description des menaces. Une stratégie de cybersécurité nationale complète doit présenter aux pays les différentes menaces sur le plan économique, et doit indiquer les programmes et les étapes à suivre ainsi que les initiatives qui doivent être mises en place pour répondre à ces menaces et protéger la connectivité Internet et les TIC utilisées par les particuliers et les entreprises publiques et privées.[19] La stratégie doit être étayée par le potentiel économique que représente l'adoption d'Internet et des TIC ; elle doit également inclure les projets qui permettront d'atténuer l'érosion du PIB provoquée par les cybermenaces et d'améliorer globalement la sécurité et la résilience des pays.

Les stratégies de cybersécurité nationales doivent refléter l'importance économique de la cybersécurité.

Concevoir une stratégie de cybersécurité nationale judicieuse ne suffit pas. Il faut pouvoir la mettre en pratique. Aujourd'hui, les principaux thèmes abordés dans la plupart des stratégies incluent : la présentation de l'autorité responsable et sa position au sein du gouvernement ; la sensibilisation et l'éducation des citoyens ; le renforcement des capacités d'intervention dans le cadre de la gestion des incidents et des crises ; l'élargissement des compétences judiciaires afin de réduire le taux de cybercrimes ; la création de partenariats entre les secteurs public et privé et la mise en place de systèmes fiables de partage et d'échange des informations; et la mobilisation de ressources permettant d'établir un programme de recherche

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

et développement et d'innovation. De nombreuses stratégies commencent par fournir des données statistiques en quantifiant le nombre d'incidents et le niveau d'endommagement des infrastructures, et en présentant les diverses menaces. Les données sont utilisées pour justifier la responsabilité organisationnelle et l'augmentation des financements destinés aux missions et aux entreprises. Ces stratégies mettent rarement l'accent sur les services et les infrastructures les plus menacés et elles n'assurent aucune harmonisation entre les mesures de sécurité et les ressources requises pour réduire cette exposition aux risques et les pertes économiques. Une stratégie de cybersécurité nationale judicieusedoit présenter le ou les problèmes stratégiques du point de vue économique, identifier l'autorité compétente chargée de la mise en œuvre de la stratégie et lui donner les moyens d'exécuter celle-ci[20] ; inclure dans un plan de mise en œuvre des objectifs spécifiques, mesurables, réalisables, basés sur des résultats et un calendrier; et reconnaître la nécessité de mobiliser un nombre de ressources limité (ex : volonté politique, argent, temps et citoyens) dans un environnement compétitif, afin d'obtenir les résultats escomptés dans les domaines de la sécurité et de l'économie.

Soixante-sept pays au moins (d'autres sont en train de le faire) ont déjà publié leur stratégie de cybersécurité et présenté les étapes clés qui permettront d'améliorer leur sécurité et résilience nationales.[21] Beaucoup d'autres pays ont mis en place des stratégies nationales (ne s'appliquant pas spécifiquement à la cybersécurité) qui permettent de concentrer et de coordonner leurs efforts visant à améliorer leur position en termes de cybersécurité. Peu de pays cependant harmonisent de manière explicite leur programme économique et leurs priorités nationales en matière de sécurité et abordent spécifiquement l'importance de la cybersécurité sur le plan économique. Et encore moins de pays élaborent des stratégies pratiques. Tous les pays ont ainsi la possibilité de revoir ou de développer leurs stratégies pour prendre en compte l'importance de la cybersécurité d'un point de vue économique.

Une stratégie de cybersécurité nationale complète doit inclure les volets suivants :

Déclaration :

A. La publication d'une stratégie de cybersécurité nationale incluant les débouchés et les risques économiques associés à l'adoption des TIC ;

Organisation :

A. La désignation d'une autorité compétente et la définition claire de son pouvoir positionnel ;

B. L'identification des principales entités gouvernementales affectées par et/ou responsables de la mise en œuvre de la stratégie de cybersécurité nationale ;

C. L'identification des entités du secteur commercial affectées par et/ou responsables de la mise en œuvre de la stratégie de cybersécurité nationale (en reconnaissant les dépendances au sein du secteur commercial) ;

Ressources :

A. L'identification des ressources financières et humaines requises et allouées dans le cadre de la mise en œuvre de la stratégie ;

B. La présentation du pourcentage du PIB que la mise en œuvre de la stratégie est censée produire (à la hausse ou à la baisse, et approximativement) ;

Mise en œuvre :

A. L'identification des systèmes requis pour protéger les cyberinfrastructures critiques et assurer l'adoption des TIC ;

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

B. L'identification des services critiques (et non pas des infrastructures critiques) que la stratégie prévoit de protéger et de rendre plus résilients ; et

C. L'identification des normes nationales relatives aux accords sur la continuité des services (24 heures sur 24, 7 jours sur 7) et des conditions de signalement des interruptions concernant chaque service, industrie et infrastructure critique.

Les conclusions obtenues pour cette rubrique essentielle, de même que pour les six autres aspects, représentent l'instantané d'un contexte dynamique en évolution constante. Au fur et à mesure que les pays continuent d'élaborer leur stratégie de cybersécurité nationale, les mises à jour de cet élément clé reflèteront ces changements et permettront de surveiller, de contrôler et d'évaluer tout développement substantiel et important. L'IPC continuera ainsi de fournir un modèle comprenant de nouveaux exemples qui aideront les autres pays à formuler ou à modifier leurs stratégies.

2. RÉPONSE AUX INCIDENTS

Le deuxième élément clé indiquant la capacité d'un pays à lutter contre la cybercriminalité concerne le renforcement et le maintien de sa capacité à intervenir efficacement en cas d'incidents observés à l'échelle nationale. Bien souvent, cette capacité est représentée par la création, au niveau national, d'une ou de plusieurs équipes d'intervention en cas d'incidents liés à la sécurité informatique (CSIRT nationales) ou d'équipes d'intervention en cas d'urgence informatique (CERT), ci-après conjointement appelées les « CSIRT ». Ces équipes sont chargées de coordonner les interventions en cas de catastrophe informatique survenant naturellement ou provoquée par l'homme et affectant des services et des infrastructures de l'information critiques.[22] Il existe actuellement cent-deux CSIRT nationales dans le monde entier et quatre autres CSIRT sont en cours de développement.[23] Les équipes CSIRT sont généralement composées d'experts en sécurité informatique et d'intervenants issus du milieu universitaire, du secteur privé et du gouvernement. En plus de fournir des compétences techniques répondant spécifiquement aux incidents informatiques d'intérêt national, ces équipes d'intervention renforcent la capacité d'un gouvernement national à comprendre et à lutter contre les cybermenaces. La mise en place d'une CSIRT nationale constitue par conséquent une composante clé de la stratégie globale adoptée par un pays pour protéger et maintenir les services et les infrastructures qui sont essentiels à la sécurité nationale et à la croissance économique.[24]

Les CSIRT nationales, contrairement aux équipes gouvernementales au sens strict, desservent un large public allant des ministères gouvernementaux aux entités publiques et privées, en passant par les citoyens. Une CSIRT nationale bien établie offre avant tout des services réactifs, c'est-à-dire la capacité à répondre aux incidents en maîtrisant et en atténuant ces incidents dès qu'ils surviennent.[25] Bien que l'aspect organisationnel spécifique des CSIRT nationales puisse varier et que les pays ne présentent pas tous les mêmes besoins et ressources, ces unités spécialisées à vocation particulière doivent fournir un ensemble de fonctions à la fois proactives et réactives ainsi que des services de prévention, d'éducation et de gestion de la qualité de la sécurité. Ces services incluent, sans toutefois s'y limiter : la mise en place d'une compréhension commune des menaces auxquelles est confronté le pays ; la publication d'alertes et de conseils sur les failles informatiques et les cybermenaces ; la sensibilisation à la cybersécurité et la promotion des meilleures pratiques ; l'identification, la détection, la maîtrise et la gestion des menaces à la sécurité et la préparation en cas d'incidents potentiels ; la coordination d'activités d'intervention en cas d'incidents ; l'analyse des incidents liés à la sécurité informatique et la transmission de retours et d'enseignements (présentés à des fins d'apprentissage commun) ; la promotion d'activités ayant pour

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

but d'améliorer la résilience ; et l'appui de la stratégie de cybersécurité nationale.

L'équipe CSIRT nationale de Singapour (SingCERT) a par exemple été créée en 1997 par l'Infocomm Development Authority (IDA) de Singapour, en collaboration avec l'Université nationale de Singapour (NUS). Elle fait depuis partie de l'Agence pour la cybersécurité (CSA) de Singapour. SingCERT a été conçue comme un centre intégré dédié aux réponses aux incidents et ayant pour fonction de faciliter la détection, la résolution et la prévention des incidents liés à la sécurité sur Internet. SingCERT fournit une assistance technique et coordonne les interventions pour les incidents de sécurité, identifie et surveille les tendances en matière d'intrusion dans des systèmes informatiques, diffuse en temps opportun des informations relatives aux menaces et communique avec d'autres organismes chargés de la sécurité afin de résoudre tout incident lié à la sécurité informatique.[26] Par ailleurs, SingCERT organise et anime activement les exercices de l'Association des Nations de l'Asie du Sud-Est (ANASE) et de l'Équipe d'intervention en cas d'urgence informatique de la région Asie-Pacifique (APCERT). En outre, Singapour possède sept membres du Forum regroupant les Équipes de sécurité et d'intervention (FIRST).

Les capacités d'intervention du Brésil comprennent une équipe nationale d'intervention en cas d'urgence informatique (CERT.BR) et trente CSIRT régionales réparties dans quatre états, toutes placées sous l'autorité du Comité directeur pour l'Internet brésilien. Ce comité est un organisme non gouvernemental incluant plusieurs intervenants clés. Il représente la principale entité qui est chargée de la défense des réseaux et des interventions en cas d'urgence au Brésil.[27] L'équipe brésilienne CERT.BR est chargée de la réponse aux incidents, de la sensibilisation à la cybersécurité, du recueil des données concernant les cybermenaces et l'intrusion dans des systèmes informatiques, et de la communication avec différents acteurs clés, notamment des CSIRT, des intervenants provenant du milieu universitaire et du secteur privé. Par ailleurs, les CSIRT brésiliennes incluent des équipes universitaires et issues des secteurs financier, militaire et gouvernemental[28].

Outre les CSIRT nationales, des entités similaires ont été créées au niveau régional pour améliorer et coordonner les activités d'intervention au sein de zones géographiques spécifiques. À titre d'exemple, l'AfricaCERT est un organisme à but non lucratif qui inclut onze pays africains et qui offre un forum dédié à la collaboration et à l'échange d'informations techniques entre les opérateurs de réseaux connectés à Internet dans la région. Les objectifs d'AfricaCERT incluent, sans toutefois s'y limiter : la promotion de la coopération parmi les CSIRT africaines afin de pouvoir gérer tout incident lié à la sécurité informatique ; une assistance dans la mise en place de CSIRT au sein des pays ne disposant actuellement d'aucune capacité d'intervention en cas d'incident ; la promotion et le soutien de programmes de prévention des incidents et d'éducation communautaire en matière de sécurité des TIC ; et la promotion du partage des informations et des meilleures pratiques en vigueur dans le domaine de la cybersécurité. De la même manière, l'APCERT comprend un réseau composé de vingt-huit CERT et d'autres experts de confiance spécialisés dans la sécurité au sein de la région. Elle a par ailleurs

La résilience des services critiques est essentielle à la sécurité nationale et à la croissance économique.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

pour objectif de renforcer la sensibilisation et les compétences liées aux incidents de sécurité informatique, et d'améliorer les capacités d'intervention dans la région Asie-Pacifique.[29] La mission de l'APCERT est d'obtenir un cyberespace « sain, sécurisé et fiable » par le biais d'une coopération mondiale. Afin de présenter efficacement les cybermenaces, le cadre organisationnel de l'APCERT est fondé sur un système de « point de contact » (POC) au sein duquel chaque pays désigne un membre APCERT qui sera le POC dans les situations d'urgence afin de permettre une réponse en temps opportun.[30] *De la même manière, l'OIC-CERT (Organisation of Islamic Cooperation - Computer Emergency Response Teams*, ou Organisation de la coopération islamique pour les équipes d'intervention en cas d'urgence informatique), qui inclut des états membres des régions Asie du Sud-Est, Asie du Sud, Moyen-Orient, Afrique et Asie centrale, s'efforce également d'améliorer la collaboration entre les CERT des états membres et l'OIC-CERT.

Outre le renforcement des capacités d'intervention en cas d'incident, les pays participent également à des exercices d'intervention sur des incidents informatiques. Ces derniers permettent à ces pays de mettre en pratique et de développer leurs compétences en matière de gestion des crises, et de vérifier l'aptitude opérationnelle d'une CSIRT à intervenir sous pression. À titre d'exemple, en novembre 2011, le pouvoir exécutif allemand a organisé sur une journée un exercice de planification et de gestion des crises, l'objectif étant d'élaborer des procédures en matière d'intervention gouvernementale en cas d'attaque pluridimensionnelle, pouvant notamment inclure : des attaques DDoS (déni de service distribué) contre des infrastructures critiques ; l'insertion de programmes malveillants (malware) au sein du système bancaire, à l'origine d'une crise pour les distributeurs automatiques et les cartes de crédit ; et l'introduction de fausses informations sur le trafic au sein du système de contrôle du trafic aérien.[31] L'Agence suédoise de services de secours (MSB), l'Autorité de la Poste et des télécommunications (PTS) et l'Institut national de défense radio (FRA) proposent également régulièrement des cours de formation coopérative destinés aux directeurs de l'Assurance des informations (CIAO) et aux employés travaillant au sein de la haute direction. La formation se termine par un exercice déterminant : la simulation d'une gestion de crise informatique qui inclut dans le processus de décision des intervenants publics et privés clés, notamment des parlementaires et des directeurs généraux d'entreprises fournissant quelques-uns des services critiques en Suède. Cet exercice souligne le manque de politiques et de textes juridiques cruciaux, tout en sensibilisant l'ensemble des participants à la cybersécurité.[32] Par ailleurs, la République tchèque a effectué en octobre 2015 un exercice de réponse aux incidents axé sur les menaces pesant sur les infrastructures critiques, mettant plus particulièrement l'accent sur les centrales nucléaires.[33] Certains pays réalisent également des exercices suite à des incidents informatiques qui ont déjà eu lieu. Le président de la Corée du Sud Park Geun-hye a par exemple ordonné à tout le personnel d'effectuer des formations et des exercices de guerre informatique suite à la découverte de l'introduction d'un programme malveillant dans plusieurs centrales hydroélectriques et nucléaires (KHNP) coréennes.[34]

Des exercices internationaux testent en outre les capacités opérationnelles de réponse aux incidents et simulent une certaine coopération entre les pays. Les États-Unis exécutent par exemple chaque semestre un exercice appelé « Cyber Storm » ayant pour but de renforcer la capacité des secteurs public et privé à lutter contre la cybercriminalité. Chaque exercice repose sur les enseignements tirés d'incidents réels afin de s'assurer que les participants aient la possibilité de réagir à des incidents informatiques de plus en plus complexes. L'exercice Cyber Storm prévu pour 2016 inclura seize états, onze pays et quatorze organismes fédéraux.[35] L'Union européenne organise également deux fois par an des exercices de réponse aux incidents informatiques appelés « Cyber Europe » incluant les états membres et des entreprises du secteur privé.[36] Lors d'un exercice informatique organisé sur 24 heures en 2014, Cyber Europe a permis à presque tous les états membres de l'Union européenne

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

de tester leurs capacités d'intervention dans le cadre de deux mille cyberattaques réelles incluant notamment des DDoS, des attaques par modification de pages web, l'exfiltration de données et des cyberattaques menées contre des infrastructures critiques.[37] En outre, l'Agence européenne de défense (EDA) et l'Organisation du Traité de l'Atlantique Nord (OTAN) réalisent également, à l'échelle régionale, des exercices de gestion des cybercrises complexes ayant pour objectif de renforcer la capacité des états membres à intervenir en cas d'incident informatique et de comprendre les dépendances transfrontalières.[38] Les États-Unis et le Royaume-Uni ont également récemment annoncé qu'ils allaient vérifier comment les centres financiers des deux côtés de l'Atlantique répondraient à une cyberattaque massive. L'exercice a eu lieu en novembre 2015 et a permis de tester la capacité d'intervention de chaque pays ainsi que la coordination et la communication des deux côtés de l'Atlantique[39].

Les CSIRT nationales peuvent également être utilisées comme un système permettant de renforcer la confiance et la coopération entre les pays. La Chine, le Japon et la Corée (trois pays ayant connu quelques tensions dans le passé) ont par exemple mis en place une réunion annuelle trilatérale entre les CSIRT pour discuter des systèmes de réponse aux cyberincidents. Ces rencontres ont aidé à stimuler la confiance et ainsi à créer une cyber-« hotline » permettant d'échanger des informations sur les principaux cyberincidents.[40]

Les capacités d'intervention en cas de cyberincident, les réunions conjointes et les exercices organisés ne représentent que quelques-uns des systèmes de base qui peuvent aider un pays à se préparer proactivement et à atténuer les répercussions d'un cyberincident majeur. Les CSIRT augmentent la rapidité d'intervention, le rétablissement et la résilience d'un pays face à des cybermenaces en réduisant l'impact économique et opérationnel global susceptible d'être observé suite à d'importantes attaques ou campagnes menées au niveau national. Quelques-unes des conditions préalables du déploiement réussi de ces équipes de réponse aux incidents incluent un personnel correctement formé et des ressources efficaces qui peuvent être rapidement déployées. Ces éléments aident les équipes de réponse aux incidents à encourager la coopération et la coordination dans le cadre de la prévention des incidents, à favoriser des réactions rapides face aux incidents et à promouvoir le partage d'informations entre les différents intervenants, à la fois aux niveaux domestique et international.

Une bonne capacité de réponse aux incidents nationale doit inclure les volets suivants :

Déclaration :

A. La publication d'un plan de réponse aux incidents en cas d'urgences et de crises ;

B. L'identification et la schématisation des dépendances intersectorielles assurant la continuité des opérations et la mise en place de systèmes de rétablissement en cas de catastrophe ;

C. Des éléments de preuve démontrant que le plan est exécuté et régulièrement mis à jour ;

D. La publication et la diffusion d'une ou plusieurs évaluations des cybermenaces nationales auxquelles sont confrontés le gouvernement, les infrastructures critiques et les réseaux de services clés ;

Organisation :

A. La création d'une CSIRT nationale visant à gérer les interventions en cas d'incidents et à desservir un vaste public au niveau national (au-delà du gouvernement et des fournisseurs d'infrastructures clés) ;

B. L'identification d'un réseau de points de contact nationaux faisant autorité pour les organismes gouvernementaux et réglementaires ;

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

C. L'identification d'un réseau de points de contact nationaux faisant autorité pour les secteurs clés qui sont essentiels à l'exploitation et au rétablissement des services et des infrastructures critiques ;

D. Le développement d'un système d'information, d'avertissement et d'alerte pouvant être utilisé par les centres d'intervention/cellules de crise nationaux/ales pour pouvoir recevoir, répondre et transmettre efficacement et rapidement tout renseignement urgent ;

Ressources :

A. L'identification des ressources financières et humaines requises et affectées pour permettre à la CSIRT nationale d'accomplir son mandat ;

B. L'identification de fonds supplémentaires pour activer et tester régulièrement le système d'information, d'avertissement et d'alerte et pour évaluer le niveau de résilience d'un pays face à des cyberincidents et des crises informatiques au moyen d'exercices de sécurité informatique organisés au niveau national ;

Mise en œuvre :

A. Une compétence éprouvée dans la maîtrise et la gestion des incidents, dans la résilience et les processus de rétablissement des services et infrastructures critiques ;

B. Une capacité éprouvée par les centres de réponse/cellules de crise nationaux/ales à répondre et à transmettre rapidement les alertes ;

C. Des éléments de preuve liés aux méthodes de recherche continue analysant les tendances ou les séries d'incidents de sécurité informatique d'intérêt national (et partageant des acteurs, des tactiques, des techniques et des procédures similaires) dans le but d'identifier des schémas d'activité ; et

D. L'élaboration et la mise en œuvre d'un système/programme permettant de tester et d'évaluer régulièrement la résilience d'une nation face aux incidents et aux crises informatiques au moyen d'exercices de sécurité informatique organisés au niveau national.

Les conclusions initiales obtenues pour cette rubrique essentielle sont basées sur les listes des CSIRT nationales fournies par la Division CERT de la Carnegie Mellon University (CMU)[41], l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[42], FIRST[43], et l'ITU. Des sources primaires et secondaires supplémentaires tels que les sites Internet des CSIRT nationales et des articles de presse associés sont consultées pour déterminer si les capacités existent et si elles sont financées. Au moment où les pays commencent à reconnaître l'importance de mettre en place des CSIRT nationales, les mises à jour apportées à cet élément crucial serviront à contrôler, à suivre et à évaluer ces projets.

3. CYBERCRIMINALITÉ ET APPLICATION DES LOIS

Le troisième élément indiquant la capacité d'un pays à lutter contre la cybercriminalité est démontré par sa détermination à protéger sa société des cybercrimes. La cybercriminalité ne représente pas uniquement un problème domestique. Elle transcende les frontières nationales et nécessite par conséquent des solutions transnationales. Les pays doivent manifester leur engagement international à protéger leur société contre les crimes informatiques. La plupart du temps, cette capacité se traduit par une participation à des forums internationaux dédiés à la recherche de solutions pour résoudre les problèmes internationaux liés à la cybercriminalité mais aussi par la mise en place d'organes juridiques et réglementaires nationaux visant à lutter contre la cybercriminalité. Les autorités juridiques et réglementaires chargées de ces activités doivent définir ce qui constitue un cybercrime et fournir aux entités gouvernementales des systèmes, une expertise et des ressources leur permettant d'enquêter sur les crimes cybernétiques et de les réprimer efficacement.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

Deux accords internationaux aident à démontrer l'engagement d'un pays en matière de protection de sa société face à la cybercriminalité : la « Convention sur la cybercriminalité » du Conseil de l'Europe et l' « Accord sur la coopération visant à garantir la sécurité internationale de l'information » de l'Organisation de Coopération de Shanghai (OCS). La « Convention sur la cybercriminalité » du Conseil de l'Europe, en vigueur depuis le 1er juillet 2004 et communément appelée la Convention de Budapest, offre un système harmonisant les lois nationales divergentes sur la cybercriminalité et favorisant une certaine collaboration dans l'application des lois.[44] L'efficacité de la Convention de Budapest est en quelque sorte limitée car elle autorise les pays signataires à mettre en œuvre de manière sélective les éléments de cette convention sur la base de conclusions qui, si elles n'étaient pas utilisées, pourraient « porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels. »[45] L' « Accord sur la coopération visant à garantir la sécurité internationale de l'information » de l'Organisation de Coopération de Shanghai, signé en 2009 et parfois appelé l'Accord de L'Ékaterinbourg, inclut des principes conformes à l'approche de la Convention de Budapest en matière de répression criminelle. Il cherche également à améliorer la base informationnelle juridique et à établir des systèmes pratiques de coopération entre les parties permettant d'assurer la sécurité des renseignements internationaux.[46] En vertu de ces traités, les pays acceptent d'adopter des lois appropriées, d'encourager la coopération internationale et de lutter contre les infractions pénales en facilitant leur détection, les enquêtes et les poursuites judiciaires, à la fois sur les plans national et international. L'IPC 2.0 fait honneur aux pays qui ont ratifié ou adopté l'un de ces traités car, en faisant ceci, ces pays présentent, conformément aux législations nationales, le devoir et une obligation spécifiques de maintenir leur engagement dans un contexte international.

Outre les systèmes internationaux mentionnés ci-dessus, d'autres approches internationales, multinationales et régionales sont actuellement mises en œuvre en matière de lutte contre la cybercriminalité internationale. À titre d'exemple, l'Assemblée générale des Nations unies (UNGA) a adopté un ensemble de résolutions liées à la cybercriminalité, telles que la résolution sur la « lutte contre l'exploitation des technologies de l'information à des fins criminelles » de 2001 et la résolution sur la « création d'une culture mondiale de la cybersécurité et protection des infrastructures critiques. »[47] Plus particulièrement, le Groupe d'experts gouvernementaux des Nations unies (GGE) incluant vingt pays a permis de faire avancer les choses lorsqu'il a accepté de coopérer dans le cadre de la poursuite des actes terroristes et de l'utilisation des TIC à des fins criminelles. Ses engagements ont été codifiés dans le rapport rédigé en juin 2015 par le GGE sur les *Développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale*.[48] L'APEC a également mis en œuvre un projet de renforcement des capacités en matière de lutte contre la cybercriminalité pour que les états membres puissent établir des structures juridiques et se donner les moyens d'enquêter sur les crimes informatiques. Dans le cadre de ce projet, les pays économiquement avancés de l'APEC soutiennent d'autres états membres en formant leurs autorités législatives et leur personnel chargé des enquêtes.[49]

L'IPC 2.0 s'appuie sur ces approches internationales, multinationales et régionales pour évaluer la capacité d'un pays à faire face à la cybercriminalité. Par ailleurs, l'IPC 2.0 inclut également des renseignements sur la cybercriminalité propres à chaque pays et provenant notamment de l'ANASE et de l'ITU.

Bien qu'une volonté de coopérer dans la lutte contre la cybercriminalité existe et que la ratification des accords de lutte contre la cybercriminalité soit importante, cela ne prouve pas nécessairement que les pays sont prêts à lutter contre la cybercriminalité. Les états doivent également s'efforcer de renforcer activement les capacités nationales en matière d'application de la loi dans le domaine de la cybersécurité. Par exemple, à l'École nationale de droit de l'Université de l'Inde à Bangalore (Inde), le Centre d'excellence consacré à la recherche, au développement et à la formation dans les domaines du droit informatique et de la police scientifique a pour

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

mission de traduire la législation en termes techniques et vice versa en proposant des séances de formation pratique et théorique aux officiers de police judiciaire, aux procureurs, aux organismes d'enquête, au personnel chargé de la cybersécurité, aux technologues, etc. Financé par le Département des technologies de l'information et de l'électronique (DeitY) du Ministère des Technologies de l'Information et de la Communication indien, ce centre offre une action de formation pratique dans un laboratoire de la police scientifique appliquée aux cyberdélits qui permet d'appréhender rapidement les problèmes les plus complexes.[50]

Un autre exemple concerne l'ouverture récente du Complexe mondial INTERPOL pour l'innovation (IGCI) créé à Singapour par l'Organisation internationale de police criminelle (INTERPOL). Ce centre permet aux responsables de l'application des lois de conclure des partenariats avec des industriels pour mettre au point de nouvelles techniques de formation et utiliser des outils innovateurs dans le but de combattre la cybercriminalité et d'améliorer la cybersécurité.[51] INTERPOL a par exemple créé un jeu de simulation pour sensibiliser les responsables chargés de l'application des lois sur l'intersection et le risque liés au « web obscure » (le Darknet) et aux crypto-monnaies. Le Darknet a donné naissance à une économie souterraine (illégale) qui vend des informations personnelles identifiables (IPI), des renseignements militaires, des études d'arme, des logiciels malveillants modulaires, des exploits « zero-day », des clés de cryptage et identifiants privés, et de nombreux autres types de données obtenues de manière illicite. Le premier exercice de simulation/formation a été réalisé par INTERPOL en juillet 2015.[52]

La réduction du nombre d'équipements réseau infectés représente un important investissement dans le cadre de la lutte contre la cybercriminalité.

La cybercriminalité et la cyberfraude représentent un impôt sur la croissance économique.

Outre le renforcement des capacités de lutte contre la cybercriminalité et d'application des lois, les états doivent également s'efforcer d'éliminer les infections informatiques affectant leurs infrastructures en réseau, également appelées « réseaux de zombies » (botnets).[53] Il est estimé qu'entre 5 et 12 % des ordinateurs à l'échelle mondiale sont actuellement infectés par des réseaux de zombies. Le FBI estime que chaque seconde, dix-huit systèmes sont infectés par un réseau d'ordinateurs zombies, entraînant à l'échelle mondiale des dommages dont le montant est estimé à 110 milliards de dollars.[54] Certains pays sont parvenus à répondre à cette menace. À titre d'exemple, le projet DarkSpace du gouvernement canadien (*Advanced Analytics and Dark Space Analysis for Predictive Indicators of Cyber Activity*) mené par Bell Canada et impliquant une équipe d'experts issus d'organismes gouvernementaux canadiens, d'institutions universitaires et d'entreprises du secteur, a présenté unplan d'entreprise pour mettre sur pied des « réseaux propres ». Cette solution permetd'éliminer les cybermenaces en fournissant un ensemble complet de preuves qui appuie proactivement les approches visant à maîtriser les menaces issues de l'Internet auxquelles est confronté le Canada. Les conclusions du projet ont permis de concrétiser ce plan d'entreprise dans le cadre d'une stratégie nationale de réduction des menaces et ont eu pour effet la création d'une Norme de cybersécurité pour les fournisseurs de services de télécommunications.[55] Un autre exemple, au Japon, concerne le Cyber Clean Center, une initiative subventionnée sur cinq ans mise en œuvre par la CERT japonaise (JPCERT) de 2006 à 2011.[56] Ce centre fut le résultat d'une collaboration transversale entre la JPCERT, différents fournisseurs de solutions de sécurité informatique et des fournisseurs de service Internet (FSI). Il a permis de créer un « réseau d'anges gardiens » automatisé assurant une protection

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

contre les infections causées par les réseaux de zombies et logiciels malveillants. Il a également offert des solutions personnalisées capables de lutter contre des programmes malveillants particuliers installés sur des ordinateurs spécifiques.[57] Les efforts déployés par le Cyber Clean Center ont été poursuivis par Telecom-ISAC Japan.[58] Enfin, iCode, un partenariat entre les secteurs public et privé mis en place en Australie par le biais de l'initiative liée à la sécurité sur Internet en Australie (AISI), a pour objectif de promouvoir chez les FSI une culture basée sur la sécurité en réduisant le nombre d'appareils affectés par une infection informatique en Australie. L'iCode encourage l'ensemble des FSI australiens à adopter l'AISI et il fournit quotidiennement aux FSI participant à cette initiative AISI des données concernant les infections par programmes malveillants et la vulnérabilité des services.[59]

La cybercriminalité et la cyberfraude représentent un impôt sur la croissance économique. Les dommages causés par la cybercriminalité ont atteint, selon des estimations, 445 milliards de dollars à l'échelle mondiale. Ils ont sur les économies nationales un impact négatif s'élevant à environ 1 % du PIB et ont engendré la perte de près de deux cent mille emplois.[60] Il est nécessaire pour l'économie d'investir dans la lutte contre la cybercriminalité et de renforcer les capacités d'application des lois. En développant les capacités d'application des lois relatives aux crimes cybernétiques par la ratification de traités, une coopération internationale, des capacités accrues, la mise en œuvre de programmes d'élimination des réseaux de zombies et d'autres initiatives, les pays pourront atténuer les cyber-risques auxquels ils sont confrontés et stimuler leur croissance économique future.

Un engagement national et international sincère en matière de protection des sociétés face à la cybercriminalité doit inclure les volets suivants :

Déclaration :

A. Un engagement national et international manifeste envers la protection des sociétés de la cybercriminalité en ratifiant des accords internationaux sur la cybercriminalité ou d'autres accords similaires ayant pour objectif de combattre les crimes cybernétiques ;

B. Un engagement manifeste envers l'établissement de systèmes juridiques et politiques nationaux pour réduire plus particulièrement les activités criminelles émanant du pays et pour promouvoir des systèmes de coordination visant à résoudre le problème de la cybercriminalité nationale et internationale ;

Organisation :

A. La mise en place d'une capacité institutionnelle complète ayant pour fonction de lutter contre la cybercriminalité, incluant notamment la formation des juges, des procureurs, des avocats, des responsables chargés de l'application des lois, des experts de la police scientifique et d'autres enquêteurs ;

B. La mise en place d'un organisme de coordination ayant pour principal objectif et mission de vérifier le respect de l'ensemble des obligations internationales liées à la cybercriminalité, sur le plan domestique et dans tous les domaines de compétences (ex : coopération transfrontalière) ;

Ressources :

A. L'identification des ressources financières et humaines requises et affectées à la lutte contre la cybercriminalité ;

B. La mise en place d'une procédure comptable permettant de déterminer le pourcentage du PIB annuel affecté par la cybercriminalité (pertes réelles en devise réelle), afin d'évaluer les échanges systémiques nationaux en termes de coûts et de bénéfices et d'allouer efficacement les ressources ;

Mise en œuvre :

A. Des preuves concrètes de l'engagement d'un pays à passer en revue et à mettre à jour ses lois exis-

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

tantes et ses systèmes de gouvernance réglementaire, à identifier ses lacunes et le recoupement des responsabilités attribuées aux autorités, et à définir et traiter en priorité les domaines nécessitant d'être mis à jour (ex : les lois existantes telles qu'une ancienne loi sur les télécommunications) ;

B. En vertu du droit national, l'institution d'infractions pénales pour les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes, réseaux et données informatiques, et pour toute utilisation illégale desdits systèmes, réseaux et données, incluant notamment les violations internationales de droit d'auteur ; et

Information sharing must be underpinned by trust and buy-in from all stakeholders.

C. Des preuves concrètes de l'efficacité d'un pays en matière de réduction du nombre d'infections informatiques provenant de ses propres infrastructures et réseaux (ex : élaboration de projets d'élimination des réseaux de zombies et des programmes malveillants).

Les conclusions initiales de cette rubrique essentielle sont basées sur une étude qui permet de déterminer si un pays a ratifié ou adopté la Convention de Budapest ou l'Accord de L'Ékaterinbourg de l'Organisation de coopération de Shanghai, et de préciser si le pays participe activement aux différentes approches régionales, multinationales ou internationales en matière de lutte contre la cybercriminalité. En outre, l'activité actuellement observée au sein des réseaux de zombies (nœuds de commande et de contrôle et nombre total d'infections informatiques) provenant du pays est utilisée pour évaluer l'efficacité des initiatives mises en œuvre pour lutter contre les réseaux de zombies. L'IPC 2.0 s'appuie sur des sources primaires et secondaires pour déterminer si un pays a mis en place des systèmes juridiques et réglementaires, d'autres actions restreignants les risques ou s'il a alloué les fonds nécessaires à la mise en œuvre positive de ces initiatives. Les mises à jour apportées à cet élément crucial serviront à contrôler, à suivre et à évaluer les développements substantiels et importants.

4. PARTAGE DES INFORMATIONS

Le quatrième élément indiquant l'aptitude d'un pays à lutter contre la cybercriminalité est sa capacité à établir et à maintenir des systèmes de partage des informations permettant l'échange de renseignements et/ou d'informations utilisables entre les gouvernements et les secteurs industriels. Les principales activités telles que l'identification, l'évaluation et la réponse aux attaques ciblées (qui peuvent avoir des répercussions considérables sur le réseau mondial de télécommunications, le commerce et le tertiaire) nécessitent bien plus que la mise en place de systèmes de surveillance et de protection traditionnels. À l'échelle mondiale, la plupart des gouvernements et des entreprises ont élaboré des programmes de partage des informations pour mieux comprendre les risques posés par les acteurs étatiques et non étatiques. Ils gèrent par ailleurs leur exposition aux différentes vulnérabilités et donc aux infections informatiques et violations qui en découlent.

Les systèmes de partage des informations officiels, similaires à certains services fournis par les CSIRT et CERT nationales, peuvent aider à favoriser la coordination en matière de réponse aux incidents, à faciliter le partage en temps réel des renseignements sur les menaces, à mieux comprendre comment les secteurs sont ciblés, à savoir quelles informations sont perdues et à connaître les méthodes possibles pour défendre les actifs informationnels. Au moins quatre différents modèles de partage des informations ont été élaborés pour répondre aux cybermenaces et pour aider les entités à protéger leurs actifs informationnels : (1) un modèle encouragé par le gouvernement ; (2) un modèle encouragé par les industriels ; (3) un modèle encouragé par un partenariat à but non lucratif ; et (4) un modèle encouragé par un

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

partenariat hybride entre les universités, le gouvernement et l'industrie. Chaque méthode présente des défis particuliers, par exemple trouver un équilibre entre le besoin d'échanger rapidement des informations sur la cybersécurité passibles de poursuites tout en protégeant la confidentialité des données et les libertés civiles, et de gérer des ressources et intérêts financiers et humains divergents. Deux facteurs sont toutefois requis pour que ces modèles puissent être efficaces : l'engagement et la confiance, qui doivent être étayés par des objectifs, des rôles, des responsabilités et des résultats clairement définis. En d'autres termes, si une partie se montre réticente ou défensive, il sera difficile de parvenir au succès.[61]

Par ailleurs, les intervenants doivent être en mesure de partager de précieux renseignements sur des incidents graves, ce qui implique de disposer d'une définition claire du type d'information qui doit être partagée, des personnes qui y auront accès et des mesures de sécurité qui devront être prises pour protéger les informations une fois qu'elles auront été émises par le détenteur initial. Le niveau de complexité de cet échange d'informations sensibles augmente proportionnellement à la taille des groupes et peut-être de manière exponentielle lorsque les membres de ces groupes sont des états souverains présentant des préoccupations différentes sur la sécurité nationale.

De nombreux pays ont déjà élaboré de solides programmes d'échange d'informations nationaux pouvant servir à d'autres pays de modèle incluant les meilleures pratiques à suivre. Ces programmes tendent à regrouper les intervenants similaires au sein d'un même groupe et à rassembler ces groupes dans un programme national. Les Pays-Bas ont par exemple créé le Centre de cybersécurité national (NCSC) (une initiative mise en œuvre par le gouvernement issue de la GOVCERT hollandaise et qui s'est transformée en un partenariat réussi entre les secteurs public et privé), chargé de la sécurité numérique et du partage des informations au sein du pays.[62] L'une de ses principales missions consiste à surveiller en permanence l'ensemble des sources (potentiellement) douteuses sur Internet et d'alerter les organisations et les autorités publiques en cas de cybermenace. Le NCSC est également directement connecté à tous les centres de partage et d'analyse des informations (ISAC) du pays et les renseignements sont partagés dans le cadre du « Protocole du Feu Rouge » (*Traffic Light Protocol*, ou TLP), qui classe les informations en quatre niveaux : rouge, jaune, vert et blanc. Le programme de partage des informations hollandais a été modelé sur celui du Centre de coordination sur la sécurité des infrastructures nationales du Royaume-Uni (NISCC), qui a fourni des conseils centrés sur la sécurité des informations aux infrastructures nationales critiques.[63] De la même manière, l'Agence japonaise pour la promotion des technologies de l'information (IPA) représente l'autorité institutionnelle chargée du partage des informations entre le gouvernement et les industries critiques. Elle a par ailleurs déjà démontré sa capacité à établir des relations de confiance avec les plus grandes entreprises du pays et à fournir rapidement des services de renseignements efficaces. En outre, l'IPA travaille étroitement avec le Ministère de l'économie, du commerce et de l'industrie (METI), le Centre de sécurité de l'information national (NISC) et l'équipe de conseil chargée de la lutte contre la cybercriminalité (J-CRAT), afin de répondre aux principaux incidents informatiques affectant les infrastructures critiques.[64]

Par ailleurs, aux États-Unis, le Centre de partage et d'analyse des informations liées aux services financiers (FSISAC) (projet encouragé par les industrielset mis en œuvre par le secteur des services financiers), facilite la détection, la prévention et la réponse aux incidents informatiques et aux activités frauduleuses. Il a établi de solides relations avec les fournisseurs de services financiers, les agences de sécurité privées, les organismes fédéraux/nationaux, étatiques, locaux et gouvernementaux, les autorités chargées de l'application des lois et autres entités de confiance, afin de rapidement fournir aux entreprises du monde entier des alertes et autres informations critiques fiables concernant les cybermenaces. Dans le cadre de ces initiatives, le FSISAC utilise un « protocole du Feu Rouge » différent pour définir les publics qui peuvent et qui doivent recevoir des informations spécifiques.[65] FSISAC élargit actuellement son service de partage des informations sur les cybermenaces à l'échelle internationale en le proposant au Royaume-Uni

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

et à l'Europe. D'autres ISAC existent également dans de nombreux secteurs mais ne sont pas aussi efficaces.

Aux États-Unis, l'Alliance nationale pour la formation et la police scientifique appliquée aux cyberdélits (NCFTA) est une société à but non lucratif dont la mission est de faciliter la collaboration entre le secteur privé, les universités et les entités chargées de l'application des lois, afin d'identifier, d'atténuer et de neutraliser les cybermenaces complexes. Outre des responsables chargés de l'application des lois aux niveaux national et local et des industriels, cette initiative mise en œuvre dans le cadre d'un partenariat à but non lucratif est également représentée au niveau international par le Canada, l'Australie, le Royaume-Uni, l'Inde, l'Allemagne, les Pays-Bas, l'Ukraine et la Lituanie. La NCFTA permet d'échanger avec les sociétés, de manière fonctionnelle et rapide, des renseignements liés aux cybermenaces ; par ailleurs, elle conclut des partenariats avec des experts spécialisés issus du public ou du privé, et des secteurs universitaire et de l'application des lois dans le but de réduire les risques et les activités frauduleuses et de rassembler les éléments de preuve nécessaires pour traduire les criminels en justice.[66]

Des informations passibles de poursuites envoyées en temps reel représentent le principal élément permettant d'atténuer les cybermenaces.

Enfin, le Centre norvégien de cybersécurité et de sécurité des informations (CCIS) de l'Université de Gjøvik est une initiative conjointe (impliquant les universités, le gouvernement et les industries) qui représente une autre approche en matière de partage des informations et de collaboration dans le cadre de la cybersécurité. Le CCIS encourage une approche nationale systématique et offre un modèle de partage des informations qui vise à protéger la capacité des sociétés à détecter, à alerter et à gérer de graves incidents cybernétiques. En outre, il soutient des travaux de recherche nationaux de qualité et le développement de solutions dans le domaine de la cybersécurité et de la sécurité des informations.

Outre les divers programmes de partage des informations actuellement élaborés par les pays, la plupart des services de renseignements et de défense des États recueillent de précieuses informations sur les cybermenaces, et certains ont même commencé à rendre public ce type de renseignements et à partager ces informations avec d'autres entités gouvernementales et industries critiques. En effet, une connaissance situationnelle en temps réel est souvent l'élément clé qui permet d'éviter ou d'atténuer des cybermenaces spécifiques. Certains pays comme le Brésil ont inventé des systèmes qui ont pour but de déclassifier (rendre publiques) des informations utilisables pour alerter d'autres organismes (publics ou privés) sur les vulnérabilités, les menaces et tactiques spécifiques, et les éventuelles solutions de défense élaborées dans le cadre de leurs projets de partage des informations.[67] Améliorer l'attitude défensive du pays est essentiel et certains pays sont prêts à déclassifier une partie de leurs renseignements pour assurer une meilleure sécurité au sein du pays.

La capacité d'un pays à échanger des informations utilisables, précises et opportunes (entre le public et le privé et au sein de chaque secteur) contribue à réduire les vulnérabilités et l'exposition au risque, permettant ainsi d'atténuer les risques qui en découlent. Au fur et à mesure que le partage de l'information se développe en termes de fréquence et de qualité, les organisationsdoivent être à même de répondre plus rapidement et plus proactivement aux cybermenaces auxquelles sont confrontées leurs infrastructures réseau. La création et la mise à jour de programmes de partage d'informations utilisables représentent un investissement essentiel à la croissance économique.

Un programme national efficace et intersectoriel permettant de partager des informations utilisables doit inclure les volets suivants :

Déclaration :

A. La formulation et la diffusion d'une politique sur le partage des informations dans les différents secteurs qui permet l'échange

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

d'informations utilisables entre les États et les divers secteurs industriels ;

Organisation :

A. L'identification d'une structure institutionnelle qui transmet des informations faisant autorité issues de sources gouvernementales à des organismes gouvernementaux et des industries critiques (de Gouvernement à Gouvernement) ;

B. L'identification d'une structure institutionnelle qui garantit l'existence de systèmes (modèles de reporting, technologie, etc.) d'échange d'informations sur les incidents transectoriels (échange bidirectionnel), à la fois sur le plan opérationnel (en temps quasi réel) et scientifique (post facto) (du Gouvernement à l'Industrie/d'industrie à industrie) ;

C. La mise en place d'un système universitaire ou à but non lucratif permettant l'échange d'informations sur les vulnérabilités, les incidents ou les solutions (modèle alternatif, par exemple, la NCFTA ou la Base de données nationale sur les vulnérabilités)[68] ;

Ressources :

A. L'identification des ressources financières et humaines requises et allouées au programme d'échange d'informations faisant autorité élaboré par le gouvernement ou à toute structure institutionnelle dédiée aux systèmes de partage des informations ;

Mise en œuvre :

A. Éléments de preuve concrets démontrant que les systèmes de coordination mis en place entre les différents secteurs et intervenants pour répondre aux interdépendances cruciales (incluant notamment une connaissance situationnelle des incidents et une gestion des incidents intersectorielle et entre les intervenants) sont correctement gérés et vérifiés afin de garantir performance et efficacité ; et

B. Des éléments de preuve concrets démontrant la capacité du gouvernement à rapidement déclassifier (rendre public) tout renseignement cybernétique utilisable et à le partager avec l'ensemble de l'Administration et les industries critiques.[69]

Les conclusions initiales de cette rubrique essentielle sont basées sur une étude permettant de déterminer si un pays a établi des systèmes de partage des informations ou tout autre mécanisme de coordination. En s'appuyant sur des sources primaires et secondaires, l'IPC 2.0 indique si de tels systèmes existent et s'ils sont financés correctement. Les mises à jour apportées à cet élément crucial serviront à contrôler, à suivre et à évaluer les principaux développements substantiels.

5. INVESTISSEMENT DANS LA RECHERCHE ET LE DÉVELOPPEMENT

Le cinquième élément indiquant la capacité d'un pays à lutter contre la cybercriminalité est l'établissement d'une priorité nationale en matière d'investissement dans la recherche fondamentale et la recherche appliquée sur la cybersécurité et, de manière plus générale, dans des projets liés aux TIC. Les progrès observés dans les TIC ont révolutionné presque tous les secteurs de l'économie. Ils ont transformé les entreprises, les gouvernements, les systèmes d'éducation et la manière dont les citoyens vivent, travaillent et se divertissent. Ces innovations favorisent la croissance économique, peuvent augmenter la résilience et créent des conditions favorables à un niveau de sécurité élevé.

Le gouvernement et les entreprises ont tous un rôle à jouer et peuvent combiner la puissance de leurs budgets de Recherche et Développement pour améliorer la prochaine génération de TIC et de technologies et solutions connectées à Internet. Les entreprises et les gouvernements adoptent l'Internet mobile, les services informatiques hébergés sur le Cloud, les mégadon-

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

nées, l'informatique quantique et l'Internet des Objets (IdO). Ils doivent en outre investir dans la fiabilité, la sécurité et la résilience de ces services et technologies numériques. En investissant dans la recherche et le développement cybernétiques et dans d'autres innovations informatiques, les pays, universités et entreprises peuvent plus facilement réduire l'écart entre leur cyberinsécurité et les capacités des pirates informatiques. Selon des estimations, le programme « Horizon 2020 » de l'Union européenne affecte par exemple 80 milliards d'euros à la recherche et aux projets de développement technologique. Dans le cadre du principe fondamental du libre accès établi par l'Union européenne, le programme a pour objectif d'augmenter les résultats en matière de recherche, d'accélérer l'innovation et l'efficacité, et d'améliorer la transparence. Horizon 2020 possède trois composantes principales. La première est axée sur les sciences fondamentales et appliquées, également connues sous l'expression « Excellence scientifique », et prévoit de financer la formation doctorale de vingt-cinq mille nouveaux doctorants au cours des sept prochaines années. La deuxième composante est axée sur le « Leadership permettant la création de technologies industrielles », qui met en avant les TIC, les nanotechnologies, les nouveaux matériaux et les systèmes de traitement des données, entre autres. La troisième composante permet de financer des solutions qui ont pour but de répondre aux problèmes socio-économiques dans des domaines tels que la santé, l'énergie, le transport et la sécurité. L'un des critères d'évaluation pour cet investissement est la coopération transnationale entre les entreprises et l'élaboration de solutions qui répondent aux besoins paneuropéens.[70]

L'innovation dans les domaines de la cybersécurité, de la recherche et du développement doit augmenter la fiabilité, la sécurité et la résilience de notre future société de l'information.

De la même manière, les États-Unis affectent en priorité plus de 4 milliards de dollars chaque année aux projets de recherche transversaux dans le cadre du programme national de recherche et de développement dans le secteur des technologies de l'information (NITRD). Les domaines de recherche prioritaires pour 2016-2020 incluent : les mégadonnées, les systèmes cyberphysiques, la cybersécurité et la recherche et le développement en matière de vie privée, les applications informatiques sophistiquées et le partage du spectre sans fil.[71] Le programme NITRD est aux États-Unis la principale source de travaux financés au niveau fédéral sur les technologies avancées de l'information liées à l'informatique, au réseautage et aux logiciels. Le programme tente d'accélérer le développement et le déploiement de technologies de l'information avancées pour améliorer la défense nationale et la sécurité intérieure mais aussi pour augmenter la productivité et la compétitivité économique des États-Unis. Par ailleurs, l'Agence pour les projets de recherche avancée de défense (DARPA), l'Initiative pour les projets de recherche avancée sur les renseignements (IARPA) et l'Agence pour les projets de recherche avancée sur la sécurité intérieure (HSARPA) disposent également de financements dédiés à la recherche et au développement cybernétiques. Néanmoins, si l'on rassemblait tous les budgets alloués à la recherche et au développement cybernétiques, le montant total équivaudrait toujours à moins d'1 % du PIB américain. Au vu du nombre considérablement élevé de cyber-risques auxquels sont actuellement (et seront) confrontés les États-Unis, ce 1 % du PIB ne sera pas suffisant pour combler les lacunes observées en matière de cybersécurité.

D'autres projets parrainés par le gouvernement encouragent l'innovation dans le domaine de la cybersécurité en offrant des primes et des incitations telles que des crédits d'impôts liés à la recherche et au développement. Par exemple, après avoir reconnu que stimuler l'investissement organisationnel nécessitait souvent des encouragements et un engagement de la part du gouvernement, Israël a récemment approuvé des allègements d'impôts considérables pour les entreprises de cyberdéfense qui intègrent et mettent en œuvre

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

des activités au sein de leur « cyberpark » national situé à Be'er Sheva.[72] En encourageant un écosystème novateur qui réunit l'industrie, le monde universitaire et le gouvernement en rapprochant physiquement des exterts techniques, Israël met en place une plate-forme de cybersécurité économique et stratégique. Le cyberpark de Be'er Sheva favorise également dans le domaine cybernétique la création de partenariats entre les entreprises publiques et privées ; il représente un centre d'excellence pour l'innovation et un centre de formation et de pôle d'emplois efficaces.

Les subventions et les bourses est un autre processus utilisé sur le marché pour améliorer la sensibilisation à la cybersécurité, développer les connaissances et augmenter les compétences. Par exemple, le programme brésilien intitulé « Science without Borders » (La science sans frontières) offre des bourses d'étude dans tous les domaines STIM (sciences, technologie, ingénierie et mathématiques), notamment pour l'informatique et les technologies de l'information. De la même manière, le Conseil national pour le développement scientifique et technologique (CNPq), organisme du Ministère des sciences, de la technologie et de l'innovation, fournit une « bourse d'initiation aux sciences » visant à encourager l'apprentissage des TIC chez les jeunes étudiants.[73]

Les plate-formes d'innovation cybernétique accélèrent la mise en pratique des idées et des technologies pour parvenir à des solutions.

Les centres d'innovation en matière de cybersécurité, tels que le Hague Security Delta (le HSD situé à La Haye), facilitent l'innovation dans les domaines de la recherche et du développement en cybersécurité et encouragent la collaboration entre les entreprises du secteur privé, les gouvernements et les instituts de recherche. Le HSD, fondation qui bénéficie du soutien de la municipalité de La Haye et du Ministère des affaires étrangères hollandais, est le plus vaste réseau de sécurité européen, possédant des connexions qui le relient aux principaux réseaux de sécurité situés aux États-Unis, au Canada, à Singapour et en Afrique du Sud. Son programme de cybersécurité inclut des initiatives telles que le Cyber Security Award (le Prix pour la cybersécurité) et le Cyber Incident Experience Lab (laboratoire pour les incidents cybernétiques). Parmi les projets actuels figurent la création d'une plate-forme sophistiquée de détection des programmes malveillants et l'élaboration de solutions permettant de détecter, de signaler et de gérer les failles cybernétiques à l'aide de scanners qualitatifs.[74]

D'autres « plates-formes d'innovation cybernétique » ont vu le jour dans la Silicon Valley, à Tel-Aviv, Boston, New York et Londres. La plate-forme d'innovation cybernétique londonienne appelée CyLon ou Cyber London fut par exemple le premier organe en Europe destiné à soutenir les start-up en cybersécurité. CyLon a pour objectif de promouvoir l'écosystème lié à l'innovation cybernétique à Londres et aide les entreprises à développer des produits associés à la sécurité de l'information.[75]

Ces divers projets de recherche et développement et plates-formes d'innovation cybernétique accélèrent la mise en pratique des idées et des technologies pour parvenir à des solutions permettant de faire évoluer le marché numérique, d'améliorer la sécurité et la résilience des infrastructures et des réseaux sous-jacents et de promouvoir le bien-être au sein de la société.

L'engagement d'un pays à consolider ses efforts en matière de recherche et développement cybernétiques, de formation et de renforcement des capacités doit inclure les volets suivants :

Déclaration :

A. engagement annoncé publiquement par le gouvernement visant à investir, au niveau national, dans la recherche fondamentale et appliquée en cybersécurité ;

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

B. Des mécanismes d'incitation annoncées publiquement (ex : crédit d'impôts pour la recherche et le développement) visant à encourager l'innovation dans la cybersécurité et la présentation des nouvelles découvertes, technologies de base, techniques, processus et outils ;

C. Des mécanismes d'incitation annoncés publiquement par le gouvernement (ex : subventions, bourses d'étude) pour encourager la formation en cybersécurité, l'acquisition de nouvelles connaissances et le développement des compétences ;

Organisation :

A. L'identification d'au moins une entité, chargée de contrôler les projets nationaux en recherche et développement pour la cybersécurité et offrant un point de contact national et international entre les différentes parties ;

B. La mise en place de programmes d'études institutionnels en cybersécurité, en sécurité de l'information ou dans des secteurs similaires associés aux technologies avancées axés sur la sécurité et la résilience de l'environnement numérique ;

C. La création d'une entité dont la mission est de mesurer et de signaler le taux de réussite des programmes gouvernementaux ou commerciaux (des stades de la recherche aux phases de conception des produits/services), en se concentrant sur les solutions qui améliorent la sécurité et la résilience de l'environnement numérique ;

Ressources :

A. L'identification des ressources financières et humaines requises et allouées à la recherche fondamentale et appliquée en cybersécurité et dans les projets associés ;

B. L'identification des ressources financières et humaines requises et allouées au transfert commercial ou gouvernemental des technologies de pointe et des innovations technologiques ;

Mise en œuvre :

A. Mise en œuvre de programmes dédiés au développement, à la diffusion et à la vulgarisation de normes techniques interopérables et sécurisées, acceptables pour et renforcées par des organismes de normalisation reconnus au niveau international ;

B. Éléments de preuve justifiant les efforts déployés par les gouvernements nationaux pour soutenir, faire évoluer et maintenir les activités de recherche et de développement en cybersécurité, comme le montre notamment le taux de conversion recherche/production (ex : pourcentage appliqué au niveau opérationnel au sein du gouvernement) et le taux de réussite des programmes gouvernementaux adoptés par le secteur privé ; et

C. Éléments de preuve justifiant les efforts commerciaux supplémentaires (ex : plates-formes d'innovation cybernétique) déployés pour soutenir, faire évoluer et maintenir les activités de recherche et de développement en cybersécurité, notamment en terme de taux de conversion recherche/production (ex : pourcentage appliqué au niveau opérationnel au sein du secteur privé) et le taux de réussite des programmes commerciaux adoptés par le gouvernement.

Les conclusions initiales de cette rubrique essentielle sont basées sur une étude permettant de déterminer si un pays investit dans la recherche et le développement cybernétiques, dans la formation, dans la production de connaissances et dans le développement des compétences, en plus du financement de projets associés de manière plus générale à la cybersécurité. En s'appuyant sur des sources primaires et secondaires, l'IPC 2.0 définit, le cas échéant, le type de mécanismes d'incitation

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

gouvernementaux déjà en place ainsi que les ressources dédiées à des initiatives similaires à celles que nous venons de présenter. Les mises à jour apportées à cet élément crucial serviront à contrôler, à suivre et à évaluer les principaux développements substantiels.

6. DIPLOMATIE COMMERCIALE

Le sixième élément essentiel en matière de lutte contre la cybercriminalité se voit à travers l'engagement d'un pays à intégrer les problèmes cybernétiques dans sa politique étrangère. À un niveau fondamental, la cyberdiplomatie tente d'identifier des solutions mutuellement acceptables aux défis communs. Les questions de sécurité informatique sont désormais présentent dans divers domaines liés aux relations internationales, notamment les droits de l'homme, le développement économique, les accords commerciaux, le contrôle de l'armement et les technologies à double usage, la sécurité, la stabilité, ou encore la paix et la résolution des conflits. Bien que les problématiques de cybersécurité se retrouvent dans tous les domaines et que la plupart des négociateurs soient des experts spécialisés dans un domaine spécifique (ex : commerce ou contrôle de l'armement), ces experts ne connaissent souvent pas suffisamment les opportunités ou les risques supplémentaires qui peuvent apparaître dans un monde connecté. Ainsi, la mise en place d'un bureau ou d'un personnel spécialisé dans la cybersécurité et dont le principal objectif est la prise en compte diplomatique des problématiques de cybersécurité doit faire partie intégrante de la politique étrangère de chaque pays.

Au vu de la lenteur de la reprise économique, de nombreux pays adoptent de nouvelles politiques économiques internationales fondées sur des accords commerciaux dans le but d'accélérer la croissance et de créer des opportunités de marché. Et pourtant, c'est dans le cadre de ces initiatives économiques que des préoccupations touchant la sécurité nationale sont en train d'être négociées sous le sceau du secret. L'Accord de partenariat transpacifique (TPP) a par exemple été conclu le 5 octobre 2015. Son objectif consistait à développer les activités commerciales et les investissements au sein des pays membres du TPP, à promouvoir l'innovation, la croissance et le développement économiques, et à soutenir la création et la préservation des emplois. Il a fallu cinq ans pour conclure cet accord, en partie à cause de problèmes liés à la cybersécurité.

À un niveau fondamental, la cyberdiplomatie s'efforce d'identifier des solutions mutuellement acceptables aux défis communs.

Les pays partenaires ne parvenaient pas à s'entendre sur des questions clés telles que les obligations liées à la protection des données personnelles et de la vie privée (ex : protection des droits de propriété intellectuelle), les souhaits en matière de localisation des données et les restrictions de contenu.

Les États-Unis et l'Union européenne sont en train de négocier un partenariat transatlantique de commerce et d'investissement (TTIP) semblable au TPP. Cet accord a pour but d'améliorer l'accès au marché, d'éliminer tout obstacle réglementaire inutile, d'établir des règles pour gérer les relations commerciales complexes entre les deux régions, de créer des emplois et de favoriser la croissance du PIB.[76] Deux des principaux problèmes qui retardent ce processus de négociation concernent la protection des données et la vie privée. Au cours des dix dernières années, l'Europe et les États-Unis ont adopté des normes communes protégeant le transfert et le stockage de toutes les données personnelles qui sont sauvegardées et/ou déplacées entre l'Union européenne et les États-Unis.[77] Toutefois, les documents divulgués par Edward Snowden ont révélé les activités des services de renseignements américains concernant d'autres gouvernements et citoyens, provoquant une perte de confiance parmi et entre les différents gouvernements. Suite à cela, de nombreux pays européens exigent la mise en place

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

de normes sur la vie privée co-adoptées au niveau étatique, de règles de cryptage et de cadres juridiques afin de pouvoir suivre l'évolution technologique et de responsabiliser les états en ce qui concerne la protection des données. Par ailleurs, une décision rendue récemment par la Cour européenne de justice a annulé les normes de protection des données de l'entente « Safe Harbor » qui avait été conclue il y a longtemps entre l'Union européenne et les États-Unis. La décision exécutive de l'accord « Safe Harbor » avait permis aux entreprises américaines de certifier elles-mêmes leur capacité à offrir une « protection adéquate » des données des utilisateurs européens conformément à la directive européenne sur la protection des données et aux droits européens fondamentaux tels que la protection de la vie privée. Bien que des négociations aient actuellement lieu pour mettre à jour l'accord Safe Harbour, aucune échéance temporelle n'a été fournie concernant la conclusion de ces dernières, compliquant encore plus les négociations entamées dans le cadre du TTIP.[78] À présent, la Chambre de commerce américaine au sein de l'Union européenne estime que l'annulation de l'accord Safe Harbour pourrait représenter pour l'Union européenne une perte s'élevant à 1,3 % de son PIB.[79]

Un autre accord de libre-échange régional, le Partenariat économique global régional (RCEP) fait actuellement l'objet de négociations entre les états membres de l'ANASE, la Chine, l'Inde, le Japon, la Corée, l'Australie et la Nouvelle-Zélande. Les seize pays membres du RCEP représentent près de la moitié de la population mondiale, près de 30 % du PIB mondial, et plus d'un quart des exportations mondiales. L'objectif du RCEP est d'éliminer les barrières commerciales, de favoriser la coopération économique et technique, de protéger la propriété intellectuelle, d'encourager la concurrence, de faciliter la résolution des conflits et d'améliorer l'accès au marché pour les exportateurs de biens et de services. Dans le cadre de ces négociations, certains pays cherchent à inclure des systèmes qui protègent leurs données, en faisant valoir un droit à la souveraineté des données à des fins de sécurité nationale.[80]

Par ailleurs, une série complète de négociations a actuellement lieu dans le domaine de la sécurité, plus particulièrement en ce qui concerne les technologies. Par exemple, le dispositif Wassenaar sur le contrôle des exportations des armes conventionnelles et des biens et technologies à double usage, qui possède quarante-et-un signataires dont les États-Unis, le Royaume-Uni, la Russie et la plupart des pays européens, a récemment mis en place des mesures pour contrer la vente de « systèmes de surveillance des communications » sur Internet et des « logiciels de détection d'intrusion » qui sont spécifiquement conçus ou modifiés pour éviter toute détection par des outils de surveillance ou pour vaincre toute contre-mesure de protection.[81] Les États ont différentes préoccupations concernant les applications à double objectif de ces technologies. À titre d'exemple, un outil d'évaluation des vulnérabilités utilise souvent des exploitations « zero day » pour identifier des failles sur les réseaux. Ces mêmes techniques peuvent être utilisées comme des armes. Par conséquent, soumettre ces technologies à des régimes de contrôle des exportations reflète la croyance selon laquelle les technologies sophistiquées peuvent vaincre les systèmes de défense nationale des pays et représenter un risque pour la sécurité nationale.

D'autres négociations et discussions diplomatiques actuellement en cours cherchent à établir une vision commune et/ou un règlement permettant d'améliorer la stabilité et la sécurité au sein de l'environnement TIC mondial. Ceci implique de consolider les systèmes de coopération pour répondre aux incidents de sécurité liés aux TIC et répondre aux demandes associées aux infrastructures TIC (ex : les activités illicites d'un pays causées par une infection par réseaux de zombies). La diplomatie est également utilisée pour définir le type de cyberactivité qui doit et ne doit pas être autorisée (ex : établissement de normes visant à responsabiliser les états, communément appelées des « cybernormes de comportement »). Le GGE des Nations Unies a par exemple récemment mis en avant le caractère mondial de l'environnement TIC, les menaces actuelles et potentielles dirigées vers la sécurité de l'information,

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

ainsi que les éventuelles mesures de coopération pouvant répondre à ces menaces. Le GGE s'est aperçu que l'adoption de la législation internationale, notamment des obligations de la Charte des Nations Unies, fournit un cadre essentiel à l'utilisation des TIC par les états. Il a accepté d'établir un cadre pour les cybernormes, les règles ou les principes régissant le comportement des états, et a mis en place des mesures de restauration de la confiance (CBM)[82]. Dans le cadre de ces CBM, le GGE a accepté de renforcer les systèmes de coopération entre les organismes d'État concernés afin de répondre aux incidents liés aux TIC et d'établir de nouveaux systèmes techniques, juridiques et diplomatiques visant à répondre aux demandes associées aux infrastructures TIC (ex : créer une CSIRT ou toute autre organisation officielle pouvant remplir ce type de mission). Plus récemment, le président américain Barack Obama et le président chinois Xi Jinping ont accepté (dans le principe) de suivre les recommandations du GGE et d'adopter les normes établies par les Nations Unies en matière de comportement en ligne, en particulier celles qui régissent le recours aux cyberattaques pour nuire aux infrastructures critiques d'autrui en temps de paix.[83]

La cybersécurité est incluse dans toutes les composantes des politiques étrangères et du commerce extérieur.

Sur la base de quelques thèmes généraux du GGE, les leaders du Brésil, de la Russie, de l'Inde, de la Chine et de l'Afrique du Sud (BRICS) ont accepté de collaborer dans le but de relever les défis communs liés à la sécurité des TIC. Ils ont convenu de partager les informations et les meilleures pratiques liées à l'utilisation sécurisée des TIC, de coordonner des mesures de lutte contre la cybercriminalité, d'établir un réseau de points de contact au sein des états membres et de promouvoir la coopération au sein des pays du BRICS en ayant recours aux CSIRT existantes. Ils ont par ailleurs encouragé la communauté internationale à concentrer ses efforts sur les CBM, sur le renforcement des capacités, sur le non-recours à la force et sur la prévention des conflits liés aux TIC.[84] En outre, en janvier 2015, la SCO a présenté à l'UNGA un nouveau code de conduite international lié à la sécurité de l'information, dont les objectifs sont d'identifier les droits et les responsabilités des états vis-à-vis de l'information, de promouvoir un comportement constructif et réactif et d'améliorer la coopération dans le but de répondre aux menaces réciproques associées aux TIC.[85] La SCO a remplacé le texte utilisé dans le Code de conduite de 2011 par celui des rapports élaborés par le GGE en 2012 et 2013 afin d'élargir la portée du Code de conduite parmi les membres du G77.

D'autres rencontres internationales ont permis d'évoquer des thèmes liés à l'économie, au développement et à la sécurité, c'est-à-dire des sujets qui présentent des objectifs spécifiques. L'ITU, par exemple, mène régulièrement des discussions internationales sur l'environnement politique, technologique et réglementaire des TIC et sur l'Internet lors de quatre de ses réunions internationales : le Sommet mondial sur la société de l'information (WSIS), la Conférence mondiale sur les télécommunications internationales (WCIT), la Conférence mondiale sur le développement des télécommunications (WTDC) et l'Assemblée mondiale de normalisation des télécommunications (WTSA).[86] Par ailleurs, l'OAS et l'IDB se sont unies afin de coopérer avec leurs états membres et de répondre systématiquement aux questions de cybersécurité classées en trois rubriques : (1) un développement favorisant à la fois l'inclusion sociale et la durabilité de l'environnement ; (2) les TIC comme outil permettant de créer des revenus et des emplois, d'offrir un accès aux entreprises et aux informations, d'encourager l'apprentissage en ligne et de faciliter les activités du gouvernement ; et (3) la sécurité de leurs infrastructures clés et des services dédiés au public.[87]

Il apparaît clairement que les problèmes liés à la cybersécurité sont évoqués lors de divers événements diplomatiques. La cybersécurité n'est pas uniquement

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

un problème de sécurité. Elle constitue un élément fondamental des politiques commerciales, étrangères et économiques et elle représente le futur potentiel de croissance économique d'un pays. Les éléments clés de la capacité d'un pays à s'engager efficacement et diplomatiquement dans la lutte contre la cybercriminalité incluent la mise en place d'un personnel formé et spécialisé, la création de structures organisationnelles spécifiques, et l'affectation de fonds aux discussions et négociations internationales sur la cybersécurité. Israël et la République tchèque ont par exemple mobilisé des « cyber-attachés » au sein de leurs ambassades situées dans les grandes villes, notamment à Washington DC et à Bruxelles.[88] Par ailleurs, dans le cadre d'un programme de sensibilisation à la cybersécurité, les États-Unis ont offert une formation d'une semaine au personnel diplomatique affecté en Asie.[89] Le développement de ces formations est de plus en plus important pour permettre à un pays de réaliser ses objectifs en matière de politiques étrangère et économique, d'activités commerciales et de croissance économique.

Une solide capacité d'engagement diplomatique en matière de cybersécurité doit inclure les volets suivants :

Déclaration :

A. L'identification de la cybersécurité comme élément clé de la politique étrangère et de la sécurité nationale (ex : par le biais de débats officiels impliquant généralement des leaders politiques et militaires de haut niveau participant à des discussions bilatérales et multilatérales) ;

B. L'identification des TIC et de la cybersécurité comme élément clé de la politique économique internationale, des négociations, des activités commerciales et des échanges ;

Organisation :

A. La mise en place d'un personnel formé et spécialisé au sein du ministère des affaires étrangères du pays ou d'un organisme équivalent, dont la principale mission inclut un engagement international actif et diplomatique en matière de cybersécurité ;

B. Une cohérence concrète entre le nombre et le niveau des employés diplomatiques spécialisés affectés au ministère des affaires étrangères dans le cadre de la lutte contre la cybercriminalité et l'engagement du pays à placer la cybersécurité et la diplomatie au cœur de ses priorités nationales ;

Ressources :

A. L'identification des ressources financières et humaines requises et allouées à l'engagement diplomatique en matière de cybersécurité ;

Mise en œuvre :

A. Une participation concrèteà la définition, à la signature et à l'application des accords internationaux, multinationaux, régionaux et/ou bilatéraux visant à identifier des solutions mutuellement acceptables pour relever les défis communs ; et

B. Des éléments de preuve concrets justifiant les efforts déployés pour influencer le processus de négociation sur le commerce et les échanges internationaux dans le cadre de l'utilisation des TIC ou des différents aspects liés aux cyberinfrastructures, aux services critiques et aux technologies, qui sont partagés aux niveaux international, régional et/ou national.

Les conclusions initiales de cette rubrique essentielle se basent sur une étude visant à déterminer si un pays a désigné explicitement ou créé un service gouvernemental, ou encore attribué à certaines personnes des responsabilités diplomatiques incluant à la fois les aspects économiques et sécuritaires des problèmes cybernétiques. L'IPC 2.0 s'appuie sur des sources

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

primaires et secondaires pour déterminer si et dans quelle mesure les ministères gouvernementaux ou les individus/employés participent aux, et influencent les négociations internationales sur les problèmes de cybersécurité. Les mises à jour apportées à cet élément crucial serviront à contrôler, à suivre et à évaluer les principaux développements substantiels.

7. DÉFENSE ET RÉPONSE AUX CRISES

Le septième et dernier élément indiquant l'aptitude d'un pays à lutter contre la cybercriminalité est la capacité de ses forces armées nationales et/ou de son organisme de défense à défendre le pays contre les menaces provenant du cyberespace. Les pays intéressés par ce type de capacité s'efforcent de former leurs forces de défense à la lutte contre les cybermenaces qui atteignent le niveau de cyberconflits critiques sur le plan national.[90]

Les pays sont plus inter connectés et plus dépendants d'Internet ce qui, par conséquent, les rend plus vulnérables face à des cyberactivités perturbatrices et destructrices. La plupart des pays ont une mauvaise position défensive face à des cyberattaques complexes. À l'échelle mondiale, le caractère connecté de la concurrence et des conflits modernes encourage les opposants responsables des cyberattaques à agir de manière latérale au sein des systèmes nationaux et à cibler les organisations commerciales et non-étatiques d'un pays. En août 2012, Saudi Aramco a par exemple subi une attaque ciblée qui a utilisé un logiciel malveillant pour détruire des données et endommager près de 75 % des infrastructures informatiques de l'entreprise.[91] Les responsables de la société ont affirmé que l'incident avait pour objectif d'affecter la production de pétrole. Quelques mois plus tard, en mars 2013, plusieurs institutions financières de Corée du Sud (notamment Shinhan Bank, la quatrième banque du pays) ont été affectées par un programme malveillant semblable à ceux qui avaient été utilisés lors de l'attaque menée contre Saudi Aramco. Les services électroniques de la banque ont été perturbés et des données ont été détruites. Les dommages économiques résultant de cet incident ont été estimés à environ 800 milliards de dollars.[92] En décembre 2014, des pirates informatiques sont parvenus à manipuler et à perturber les systèmes de contrôle d'une aciérie allemande, entraînant la fermeture incorrecte de son haut fourneau et provoquant ainsi d'importants dommages.[93] La même année, Sony Pictures a été victime d'une cyberattaque lors de laquelle des films cinématographiques non commercialisésont été copiés illégalement, des emails de la société ont été volés puis divulgués, et des documents financiers ont été dévoilés. Des données sensibles concernant plusieurs dizaines de milliers d'employés de Sony ont été copiées et près de 80 % des biens informatiques de l'entreprise ont été détruits (données et matériel informatique) par ce virulent malware.[94]

Les cyberactivités perturbatrices et destructives nécessitent la mise en place d'un système de cyberdéfense fiable.

Les pays doivent être en mesure de défendre leurs actifs (qu'il s'agisse de biens connectés ou en réseau) dans le cadre de conflits actuels et potentiels. La rapidité et l'expansion d'Internet permettent de mettre en relation toute les facettes de la société et fournissent un accès rapide aux cyberarmes de type militaire, offrant un avantage asymétrique à de nombreux pays. En effet, la diversité des acteurs malveillants (ex : militants politiques, criminels, terroristes, acteurs étatiques et non-étatiques, présentant tous des motifs différents) souligne le besoin de se préparer aux pires scénarios. Actuellement, plus de soixante pays possèdent des capacités en

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

matière de cyberespionnage et de lutte contre les cyberattaques, et ils s'efforcent d'acquérir et de developper des capacités défensives, préventives et offensives.[95] Par ailleurs, des pays commencent à élaborer différents outils et stratégies pour améliorer leurs systèmes de cyberdéfense au niveau national. La plupart des gouvernements cherchent instinctivement à augmenter la capacité de défense actuelle de leurs organismes chargés de la sécurité qui sont déjà capables d'agir dans le cyberespace au-delà des frontières nationales (ex : l'organisation de défense ou les services de renseignements). D'autres tentent de mettre en place ces capacités dans des organismes de sécurité qui ne se trouvent pas directement au sein de leur structure militaire.[96]

En 2010 par exemple, les États-Unis ont créé une unité militaire spécialisée (l'Unité de cybercontrôle américaine, ou United States Cyber Command) afin de défendre le pays contre les cybermenaces visant les infrastructures militaires. Sa mission a été élargie en 2015 lorsque le Ministère de la défense (DoD) a publié sa deuxième stratégie de lutte contre la cybercriminalité dans le but de faciliter le développement des cyberforces du DoD (sous la commande et le contrôle de l'Unité de cybercontrôle américaine) et de renforcer son système de cyberdéfense et sa position en matière de dissuasion face aux cybermenaces. Cette nouvelle stratégie souligne à quel point il est important d'être « capable de défendre la sécurité du territoire et les principaux intérêts américains face à des cyberattaques perturbatrices et destructrices qui pourraient avoir des conséquences dramatiques », et d'élaborer, de conserver et d'utiliser des options fiables en matière de lutte contre la cybercriminalité pour éviter toute intensification de conflit et pour façonner l'environnement à tous les stades du conflit.[97]

De la même manière, en décembre 2014, la Fédération russe a publié sa nouvelle doctrine militaire qui met en avant le développement de ses moyens de guerre électronique, à des fins à la fois offensive et défensive, mais aussi ses capacités de « dissuasion nucléaire ».[98] Le Livre Blanc rédigé en 2011 par le Ministère de la défense russe et intitulé « Vues conceptuelles sur les activités des Forces armées de la Fédération russe dans l'espace d'information » cadre parfaitement avec certains aspects de la doctrine défensive de la Russie, mais il inclut également de manière explicite l'opinion publique et la nécessité de tenir les médias au courant de l'évolution des situations conflictuelles dans le but d'éviter toute intensification de ces conflits.[99] D'après les médias russes, les leaders russes prévoient de publier en 2016 une nouvelle doctrine sur la sécurité de l'information, qui est supposée proposer le développement des forces de défense dans le cadre de la guerre des informations et des systèmes d'information à des fins de dissuasion stratégique et de prévention des conflits.[100]

La République de Corée du Sud et le Brésil ont également créé des organisations militaires semblables dans le but de protéger les capacités offensives, défensives et d'intervention, mais aussi pour garantir une victoire complète en cas de guerre électronique.[101] La Corée du Sud élargit ses capacités de lutte contre la cybercriminalité et est supposée former plus de quatre cent nouveaux « cybersoldats » au sein de son unité de cybercontrôle, pour arriver à un total de mille personnes.[102]

Par ailleurs, bien que la République populaire de Chine n'ait publiquement émis aucune doctrine stratégique officielle en matière de cyber-applications ou d'informations militaires, elle a publié des directives stratégiques militaires qui offrent des conseils sur la politique de défense.[103] Le Livre Blanc rédigé en 2013 par la République populaire de Chine et intitulé « Emploi diversifié des Forces armées chinoises » et l'ouvrage de 2014 intitulé « Opinion sur un nouveau renforcement des systèmes de sécurité de l'information », mettent en avant le développement des moyens de défense face aux crimes cybernétiques. Ces documents soulignent que l'Armée populaire de libération (PLA) ne procèdera à aucune attaque sauf si elle est attaquée, mais qu'en cas d'attaque, elle répliquera dans le cyberespace.[104]

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

Un organisme de défense cybernétique ne doit pas être un organisme uniforme au sein des Forces militaires de la nation. La police nationale et les services de renseignements peuvent être les éléments clés de la défense d'un pays dans le cyberespace, bien que les forces armées doivent également être modernisées et prêtes, sur le plan cybernétique, à affronter des conflits plus traditionnels. L'Islande a par exemple placé tous ses moyens de lutte contre les attaques cybernétiques en dehors de ses Forces armées. Dans le passé, en Islande, les responsabilités en matière de cybersécurité étaient réparties de manière officieuse entre le Ministère de l'intérieur, l'Autorité de la Poste et des télécommunications, l'Autorité de protection des données et la police islandaise. Pourtant en 2015, l'Islande a centralisé l'ensemble de ses capacités cybernétiques en les plaçant sous la responsabilité du commissaire national de la police islandaise.[105] La cyberstratégie nationale élaborée en Islande en juin 2015 souligne également le rôle intégral de l'alliance de l'OTAN en matière de cyberdéfense sur le territoire islandais.[106]

Enfin, bien qu'Israël ne dispose actuellement d'aucune « unité de cybercontrôle » officielle, le pays possède tout de même des capacités en matière de cybersécurité, qui sont réparties au sein des Forces de défense israéliennes (IDF) et de la Direction du renseignement militaire. La Direction du renseignement militaire gère les capacités offensives tandis que les services de renseignements assurent la protection. Shin Bet, le service de sûreté intérieure d'Israël, est chargé de défendre les systèmes gouvernementaux et les infrastructures nationales critiques, et l'unité opérationnelle cybernétique nationale protège les réseaux critiques et les industries privées contre les tentatives de piratage et d'espionnage.[107] Ceci est toutefois amené à changer car en juin 2015, le lieutenant-général Gadi Eisenkot, commandant de l'armée israélienne, a déclaré son intention de créer un nouveau corps d'armée au sein des IDF (dans la marine et les forces aériennes) chargé de l'ensemble des cyberactivités. Dans le cas où le ministre de la défense approuverait ce nouveau corps d'armée, les nouvelles IDF seront opérationnelles dans deux ans. Une fois opérationnelle, la nouvelle unité de cybercontrôle intègrera les moyens de défense actuellement fournis par les IDF et les capacités offensives et les services de renseignements seront assurés par l'Unité 8200 et d'autres groupes militaires chargés des services de renseignements.[108] Ce projet respecte le nouveau programme élaboré pour les IDF sur cinq ans appelé « Gideon », qui a été publié en août 2015. « Gideon » demande spécifiquement l'augmentation du nombre d'initiatives mises en œuvre pour lutter contre les cyberattaques et autres menaces asymétriques émanant de groupes non-étatiques et terroristes dans la région.[109]

Des capacités de cyberdéfense sont essentielles pour permettre à un pays d'assurer sa sécurité nationale et économique. Plus les pays deviennent dépendants de l'Internet et des systèmes TIC, plus ils deviennent vulnérables face aux cybermenaces « de bas niveau » et aux activités asymétriques. Les pays se retrouvent dans un cercle vicieux : l'adoption des TIC est essentielle à leur croissance mais plus un pays est connecté aux nouvelles technologies, plus il se retrouve confronté à un certain nombre de risques. Rester à l'écart de l'économie de l'Internet n'est désormais plus une solution. Les pays doivent être prêts à se défendre dans le cyberespace. Si un pays est incapable de se défendre, il n'est pas en mesure de lutter contre la cybercriminalité.

L''engagement d'un pays à créer et à déployer des unités de défense nationales spécialisées dotées de responsabilités et de moyens de défense face aux attaques cybernétiques doit inclure les volets suivants :

Déclaration :

A. La publication de déclarations nationales qui attribuent à une organisation la responsabilité de la cyberdéfense nationale, une mission qui se trouvera au cœur de ses priorités ;

B. La mise en œuvre de politiques permettant à

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

l'organisme de cyberdéfense de répondre aux cybermenaces ;

C. La formulation de déclarations nationales ordonnant à l'organisme de cyberdéfense de développer des capacités permettant de répondre aux menaces au sein ou à l'extérieur du territoire souverain ;

Organisation :

A. La création, au niveau national et dans le secteur militaire, d'une organisation dont la principale mission est d'assurer la cyberdéfense de la nation ;

B. La création, au niveau national et en dehors du secteur militaire, d'une organisation dont la principale mission est d'assurer la cyberdéfense de la nation ;

Ressources :

A. L'identification des ressources financières et humaines requises et allouées à la création, dans le secteur militaire, d'une organisation dont la mission inclut explicitement la cyberdéfense de la nation ;

B. L'identification des ressources financières et humaines requises et allouées à la création, en dehors du secteur militaire, d'une organisation dont la mission inclut explicitement la cyberdéfense de la nation ;

Mise en œuvre :

A. Éléments de preuve démontrant les exercices réalisés au niveau gouvernemental pour justifier les capacités nationales en matière de cyberdéfense ;

B. Éléments de preuve démontrant les exercices impliquant les entités commerciales affectées, qui sont réalisés au niveau national pour justifier les capacités nationales en matière de cyberdéfense ;

C. Éléments de preuve démontrant les exercices réalisés avec des partenaires internationaux (ex : défense mutuelle de l'OTAN ou exercice de l'APCERT) pour justifier la coopération à travers l'échange d'informations et l'entraide ;

D. L'établissement de normes favorisant un comportement étatique responsable au sein du cyberespace, et l'identification de seuils qui permettent un engagement envers la cyberdéfense ; et

Aucun pays n'est actuellement capable de lutter contre la cybercriminalité.

E. La mise en place de dispositifs d'aide rapide (distincts des CERTS ou des groupes équivalents) à la disposition du gouvernement ou de certaines industries en cas de cyberincidents graves.

Les conclusions initiales de cette rubrique essentielle sont basées sur une étude permettant de déterminer si un pays a officiellement déclaré la mise en place de forces de défense dont la mission prioritaire est la cyberdéfense de la nation. L'IPC 2.0 s'appuie sur des sources primaires et secondaires afin de déterminer le niveau de capacité opérationnel. Les mises à jour apportées à cet élément crucial serviront à contrôler, à suivre et à évaluer les principaux développements substantiels.

CONCLUSION

Les menaces auxquelles sont confrontés nos systèmes et infrastructures en réseau sont bien réelles. Elles ne cessent d'augmenter et représentent un

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

coût économique pour les pays et les sociétés. Les programmes économiques et de sécurité nationale doivent être harmonisés afin d'instaurer une certaine transparence dans le domaine de la cybersécurité. Dévoiler cette association étroite suscitera peut-être un intérêt national et mondial qui permettra d'atténuer cette érosion économique. La méthodologie complète, comparative et basée sur l'expérience de l'IPC 2.0 fournit un plan permettant d'évaluer l'engagement et la capacité d'un pays à protéger ses infrastructures et services électroniques nationaux dont dépendent sa croissance et son avenir numérique.

Le plan de l'IPC 2.0 identifie plus de soixante-dix indicateurs de données uniques concernant sept éléments essentiels : la stratégie nationale, la réponse aux incidents, la cybercriminalité et l'application des lois, le partage des informations, l'investissement dans la recherche et le développement, la diplomatie commerciale ainsi que la défense et la réponse aux crises. Ces indicateurs et ces éléments essentiels fournissent un cadre pouvant aider un pays à renforcer sa position en matière de sécurité et ainsi à lutter contre l'érosion de son PIB. En fait, l'IPC 2.0 remet en question l'idée reçue selon laquelle la cybersécurité est principalement un problème de sécurité nationale. L'IPC 2.0 peut démontrer comment la sécurité nationale est étroitement liée à la connectivité Internet et à une adoption rapide des TIC qui, une fois sécurisées, peuvent contribuer à la croissance économique et à la prospérité.

Au lieu de simplement étudier le problème, l'IPC 2.0 fournit également un cadre permettant à un pays d'évaluer son aptitude à empêcher l'érosion économique causée par la cyberinsécurité. L'IPC 2.0 sera régulièrement mis à jour avec l'ajout de critères d'évaluation sans pour autant perdre la validité des données de comparaison obtenues lors des précédentes évaluations. De cette manière, l'IPC 2.0 pourra présenter les progrès et l'évolution des pays en matière de protection des infrastructures et des services électroniques dont dépendent leur croissance et leur avenir numérique.

Aucun pays ne peut se permettre une cyberinsécurité ni de subir les pertes que celle-ci entraîne. Les données et la méthodologie de l'IPC 2.0 peuvent aider les leaders nationaux à tracer la voie vers une économie plus sûre et plus robuste dans un monde fortement axé sur les nouvelles technologies, extrêmement compétitif et en permanence menacé par les conflits.

Pour plus d'informations ou pour fournir des données relatives à la méthodologie de l'IPC 2.0, veuillez contacter :

CyberReadinessIndex2.0@potomacinstitute.org

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

BIBLIOGRAPHIE

1. Le document intitulé « Indice de préparation à la lutte contre la cybercriminalité – Version 2.0 » s'inspire de la précédente version intitulée « Indice de préparation à la lutte contre la cybercriminalité – Version 1.0 » qui a fourni un cadre méthodologique permettant d'évaluer la capacité à lutter contre la cybercriminalité au moyen de cinq éléments essentiels, à savoir : la stratégie de cybersécurité nationale, la réponse aux incidents, la cybercriminalité et le pouvoir juridique, le partage des informations ainsi que la recherche et le développement cybernétiques. L' « Indice de préparation à la lutte contre la cybercriminalité – Version 1.0 » a appliqué cette méthodologie à un premier groupe detrente-cinq pays. Pour plus d'informations sur le document « Indice de préparation à la lutte contre la cybercriminalité – Version 1.0 », consulter l'ouvrage de Melissa Hathaway intitulé « Cyber Readiness Index 1.0 » (Indice de préparation à la lutte contre la cybercriminalité – Version 1.0), *Hathaway Global Strategies LLC* (2013), *http://belfercenter.ksg.harvard.edu/files/cyber-readiness-index-1point0.pdf*.

2. L'implication des infrastructures Internet est la ' dépendance envers la connexion à Internet pour offrir des prestations de services clés tels que l'approvisionnement en eau et en électricité, le transport, la communication, la santé, etc. Pour plus d'informations sur l'implication des infrastructures Internet, consulter l'ouvrage de Melissa Hathaway intitulé « Connected Choices: How the Internet Is Challenging Sovereign Decisions », American Foreign Policy Interests 36, no. 5 (Novembre 2014): 301.

3. Parmi les exemples de stratégies économiques reposant sur les TIC qui sont mises en œuvre à l'échelle mondiale : *Digital Single Market (Europe) ; Digital India (ID) (Inde) ; Internet Plus (+) (Chine) ; et Connect 2020 (ITU)*.

4. Conseil d'État de Chine, « Internet Plus », *Guo Fa* 40 (2015). Traduit par le Département d'État des États-unis.

5. Gouvernement indien, « Programme Pillars », *Digital India: Power to Em- power, http://www.digitalindia.gov.in/content/programme-pillars*.

6. Commission européenne, « Digital Single Market: Bringing down the barriers to un- lock online opportunities », *http://ec.europa.eu/priorities/digital-single-market/*.

7. Melissa Hathaway et Francesca Spidalieri, « Sustainable and Secure Development: A Framework for Resilient Connected Societies », dans *Observatory of Cyber Security in Latin America and the Caribbean* (Décembre 2015 – Organisation des États américains).

8. Banque mondiale, « Overview », *Information & Communication Technologies Program (Programme sur les technologies de l'information et de la communication)*, dernière modification le 2 octobre 2014, *http://worldbank.org/en/topic/ict/overview*.

9. David Dean et al., « The Digital Manifesto: How Companies and Countries Can Win in the Digi- tal Economy », *Boston Consulting Group report* (Janvier 2012): 2.

10. Peter C. Evans et Marco Annunziata, « Industrial Internet: Pushing the Boundaries of Minds and Machines », *General Electric* (26 novembre 2012): 13.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

11. Melissa Hathaway, « Cyber Readiness In- dex 2.0 & Lessons Learned in the Design of national Cyber Security Strategies », (présentation réalisée au cours de l'atelier régional de l'OAS-IDB sur les politiques de cybersécurité, Washington D.C., 23 octobre 2014).

12. Frontier Economics London, *« Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy: A Report commissioned by Business Action to Counterfeiting and Piracy »*, (Londres, Frontier Economics Ltd., 2011): 47.

13. Le Bureau national de la recherche asiatique, « The IP Commission Report: The report of the commission on the theft of American intellectual property », *Bureau national de la recherche asiatique* (Mai 2013).

14. Melissa Hathaway, « Connected Choices: How the Internet Is Challenging Sovereign Decisions », *American Foreign Policy Interests* 36, no. 5 (Novembre 2014): 301.

15. Harvey Poppel est considéré comme l'inventeur des *Harvey Balls* dans les années 70, à l'époque où il occupait un poste de consultant chez Booz Allen Hamilton.

16. Sur la base des classements de PIB publiés par la Banque mondiale en 2013.

17. OCDE, *OECD Digital Economy Outlook 2015* (Paris, France : OECD Publishing, 2015), *http://dx.doi.org/10.1787/9789264232440-en*.

18. Melissa Hathaway, « Transparency, Trust, and Our Internet », (présenta- tion réalisée lors de la conférence GTEC, Ottawa, Canada, 20 octobre 2015).

19. L'adoption des infrastructures TIC inclut les segments de marché fixe et mobile (voix et données), concernant à la fois les abonnements et l'accès aux données des foyers, ainsi que l'investissement dans le secteur des télécommunications et les revenus générés par celui-ci.

20. Une autorité compétente est une personne ou une organisation à qui on a légalement délégué l'autorité, la capacité ou le pouvoir de remplir une fonction spécifique.

21. Union internationale des télécommunications, « National Strategies », *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx*.

22. Les termes CSIRT et CERT font référence à une équipe d'experts en sécurité informatique qui ont été désignés pour répondre aux incidents de sécurité informatique. Ces deux termes sont utilisés de façon interchangeable, mais « CSIRT » est le terme le plus précis.

23. L'Union internationale des télécommunications, « CIRT Programme », *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx*.

24. John Haller, Samuel Merrell, Matthew Butkovic et Bradford Willke, *« Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0 »* (Pittsburgh, PA : Software Engineering Institute, Carnegie Mellon University, 2011), *http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9999*.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

25. Olaf Kruidhof, « Evolution of National and Corporate CERTs – Trust, the Key Factor », dans *Best Practices in Computer Network Defense: Inci- dent Detection and Response*, édit. Melissa E. Hathaway, (Amsterdam : NATO Science for Peace and Security Series, IOS Press, Février 2014).

26. Équipe d'intervention en cas d'urgence informatique de Singapour, « FAQ », *https://www.csa.gov.sg/singcert/about-us/faqs*.

27. Ministério das Comunicações, « Portaria Interministerial N 147, de 31 de Maio de 1995 », *http://cgi.br/portarias/numero/147*.

28. *cert.br, «* About *CERT.br », http://www.cert.br/about/*.

29. « Documents », APCERT. *APCERT.org*, 13 octobre 2015. *http://www.apcert.org/documents/index.html*.

30. « Asia Pacific Computer Emergency Response Team Operational Framework », APCERT. *APCERT.org*, 13 octobre 2015. *http://www.apcert.org/documents/pdf/OPFW(26Mar2013).pdf*.

31. Melissa Hathaway, « Best Practices in Computer Network Defense: Incident Detection and Response », Global Cyber Security Center (Septembre 2013): 12.

32. Ingvar Hellquist (Colonel à la retraite), Conseiller principal et Lars Nicander, Directeur, Centre d'étude sur les menaces asymétriques, Université de défense suédoise, « CATS Course and Cyber Exercise », (entretien réalisé par Melissa Hathaway à Stockholm en Suède le 17 octobre 2012) et Collège de défense nationale suédois, « CATS Newsletter », *CATS Center for Asymmetric Threat Studies* (Printemps 2013).

33. Dusan Navratil, Directeur, Autorité de sécurité nationale de la République tchèque, et Robert Kahofer, Assistant spécialisé, « Cyber Czech 2015 - National Technical Cyber Security Exercise », (entretien réalisé par Melissa Hathaway à Washington DC, en octobre 2015).

34. « South Korea says Nuclear Worm is nothing to worry about », *TheRegister. co.uk*, 30 décembre 2014, *http://www.theregister.co.uk/2014/12/30/south_korea_says_nuclear_worm_is_nothing_to_worry_about/* et « Activists Hack KNHP's computer systems », World Nuclear News, 22 décembre 2014, *http://www.world-nuclear-news.org/C-Activists-hack-KHNPs-computer-systems-2212141.html*.

35. Département de la sécurité intérieure, « Cyber Storm: Securing Cyber Space », *http://www.dhs.gov/cyber-storm-securing-cyber-space*.

36. Commission européenne, « Cyber Strategy of the European Union: An Open, Safe, and Secure Cyberspace », *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, (Juillet 2013): 7 et Agence européenne chargée de la sécurité des réseaux et de l'information, « Cyber Europe », *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe*.

37. Doug Drinkwater, « Hundreds of companies face two thousand cyber-attacks in EU exercise », Magazine SC, 31 octobre 2014 dans ENISA, « ENISA Cyber Europe 2014: Media Coverage », *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information/cyber-europe-2014-media-coverage*.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

38. Agence de défense européenne, « Complex Cyber Crisis Management Exercise in Vienna », 16 septembre 2015, *https://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/09/16/complex-cyber-crisis-management-exercise-in-vienna* et OTAN, « Largest ever NATO cyber defence exercise gets underway », 21 novembre 2014, *http://www.nato.int/cps/en/natohq/news_114902.htm?selectedLocale=en*.

39. Katie Bo Williams, « US, UK to test finance sector cybersecurity this month », The Hill, 2 novembre 2015, *http://thehill.com/policy/cybersecurity/258827-us-uk-to-test-finance-sector-cybersecurity-this-month*.

40. CNCERT/CC, « 2nd China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response was held in Korea », *www.cert.org.cn/publish/english/55/2014/20140916145739295996084/20140916145739295996084_.html*.

41. Carnegie Mellon University, « List of National CSIRTs », Division CERT, *http://www.cert.org/incident-management/national-csirts/national-csirts.cfm*.

42. Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), « ENISA- CERT Inventory: Inventory of CERT teams and activities in Europe », ENISA Version 2.16 (Juin 2014), *http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe*.

43. Forum regroupant les équipes de sécurité et d'intervention (FIRST), « FIRST Members », *http://www.first.org/members/teams*.

44. Conseil de l'Europe, *Convention on Cyber- crime* (23 novembre 2001) et Organisation de coopération de Shanghai, *Cooperation in the Field of Information Security*, Séance plénière 61 (16 juin 2009).

45. *Ibid*.

46. Organisation de Shanghai Cooperation, *Cooperation in the Field of Information Security*, Séance plénière 61 (16 juin 2009), *https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf*.

47. Juge Stein Schjolberg et Amanda M. Hubbard, « Harmonizing National Legal Approaches on Cybercrime », Union internationale des télécommunications (1er juillet 2005): 6.

48. Les vingt pays qui ont signé le rapport du GGE incluent : la Biélorussie, le Brésil, la Chine, la Colombie, l'Égypte, l'Estonie, la France, l'Allemagne, le Ghana, Israël, le Japon, le Kenya, la Malaisie, le Mexique, le Pakistan, la Corée, la Russie, l'Espagne, le Royaume-Uni et les États-Unis. Voir le document des Nations Unies intitulé « Rapport du groupe d'experts gouvernementaux sur le développement dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale », A/65/201 et A/68/98 (26 juin 2015).

49. Ernesto U. Savona, « Crime and Technology: New Frontiers for Regulation, Law Enforcement, and Research » (Dordrecht, Pays-Bas : Springer, 2004): 50.

50. Advanced Centre for Research, Development and Training in Cyber Laws and Fo- rensics, « Academic Programs », *École nationale de droit de l'université de l'Inde, https://www.nls.ac.in/index.php?option=com_content&view=article&id=502&Itemid=32*.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

51. INTERPOL, « The INTERPOL Global Complex for Innovation », obtenu le 17 septembre 2015, *http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation*.

52. Madan M. Obero, « Dark Web and Crypto-Currency », (présentation réalisée lors du Cyber 360: A Synergia Conclave, Ban- galore, Inde, 30 septembre 2015).

53. Un robot-réseau est un logiciel malveillant pouvant utiliser un ordinateur pour envoyer des spams, héberger des sites de hameçonnage ou usurper une identitié en observant les frappes effectuées sur un clavier. Les ordinateurs infectés sont ensuite contrôlés par des tierces parties et peuvent être utilisés pour mener des cyberattaques. Pour plus d'informations, consulter l'ouvrage rédigé par Melissa Hathaway et John Savage intitulé « Stewardship of Cyberspace: Duties of Internet Service Providers », Cyber Dialogue 2012 (Mars 2012).

54. Alastair Stevenson, « Botnets infecting 18 systems per second, warns FBI », V3.cok.uk, 16 July 2014, *http://www.v3.co.uk/v3-uk/news/2355596/botnets-infecting-18-systems-per-second-warns-fbi*.

55. Bell Canada et al., « The Dark Space Project », *Security Telecommunications Advisory Committee* (2011): 13, *https://citizenlab.org/cybernorms2012/cybersecurityfindings.pdf*.

56. Yurie Ito, « Cyber Clean Center », (entretien réalisé à distance avec l'équipe du *Cyber Readiness Index*, Washington DC, 10 novembre 2015).

57. Ministère des affaires intérieures et des communications et Ministère de l'économie, du commerce et de l'industrie, « What is the Cyber Clean Center », *Cyber Clean Center, https://www.telecom-isac.jp/ccc/en_index.html* et Michael M. Losavio, J. Eagle Shutt, et Deborah Wilson Keeling, « Changing the Game: Social and Justice Models for Enhanced Cyber Security », dans Tarek Saadawi, Louis H Jordan Jr., et Vincent Boudreau : Cyber Infrastructure Protection, Volume II (U.S. Army War College, Strategic Studies, 2013): 101.

58. Telecom-ISAC Japan, « Chairman's Message », 12 mai 2011, *https://www.telecom-isac.jp/english/index.html*.

59. Initiative liée à la sécurité sur Internet en Australie (AISI), « Overview of the Australian Internet Security Initiative », *http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative*.

60. McAfee, « McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies », 9 juin 2014, *http://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx* et le Bureau national de recherche asiatique : « IP Commission Report: The report of the commission on the theft of American intellectual property » (Mai 2013).

61. Melissa Hathaway, « Why Successful Partnerships are Critical for Pro- moting Cybersecurity », The New New Internet, 7 mai 2010.

62. Ministère de la sécurité et de la justice hollandais, « National Cyber Security Centre (NCSC) », *https://www.ncsc.nl/english*.

63. En février 2007, le Centre national britannique de coordination pour la sécurité des infrastructures (NSAC) a fusionné avec le Centre de conseils sur la sécurité nationale (CPNI). Pour plus d'informations sur le CPNI, consulter le : Center for Protection of National Infrastructure, *http://www.cpni.gov.uk*.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

64. Agence de promotion des technologies de l'information (IPA), Japan IT Security Center, *Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) Annual Activity Report FY2012*, (Avril 2013).

65. Centre d'analyse et de partage des informations sur les services financiers, « Overview of the FS-ISAC », obtenu le 17 septembre 2015, *https://www.fsisac.com/sites/default/files/FS-ISAC_Overview_2011_05_09.pdf*.

66. National Cyber-Forensics & Train- ing Alliance, « Become a NCFTA Partner », *https://www.ncfta.net/become-ncft-partner.aspx*.

67. Raphael Mandarino, « MT2: Private Public Partnership », Cabinet de la sécurité institutionnelle, Département de la sécurité de l'information et des communications, Bureau du Président, (présentation effectuée lors de la 1ère conférence sur la sécurité organisée par INTERPOL à Hong Kong, du 15 au 17 septembre 2010).

68. National Institute for Standards and Technology, « National Vulnerability Database », *https://nvd.nist.gov*.

69. Le Royaume-Uni et le Brésil ont mis en place des systèmes permettant de déclassifier (rendre publics) les renseignements et de les partager avec les secteurs critiques. Ces systèmes sont considérés bien meilleurs que les systèmes américains.

70. Commission européenne, « ICT Re- search & Innovation », *Horizon 2020: The EU Framework Programme for Research and Innovation, http://ec.europa.eu/programmes/horizon2020/en/area/ict-research-innovation*.

71. Pour plus d'informations sur le NITRD (Networking and Information Technology Research and Development Program) et sur ses domaines de recherche, consulter : *www.nitrd.gov/Index.aspx* and NITRD, « The Networking and Information Technology and Research Development Program », *Supplement to the President's Budget FY 2016* (Février 2015), *https://www.whitehouse.gov/sites/default/files/microsites/ostp/fy2016nitrdsupplement-final.pdf*.

72. Consulat général d'Israël à New York, « Cabinet approves tax break for National Cyber Park », Consulat général d'Israël à New York, 7 juin 2014, *http://embassies.gov.il/wellington/NewsAndEvents/Pages/Cabinet-approves-tax-break-for-National-Cyber-Park-6-Jul-2014.aspx*.

73. Ciência Sem Fronteiras, « FAQ », *http://www.cienciasemfronteiras.gov.br/web/csf-eng/faqEGTI_2013*-2105_v1-3, Coordination pour l'amélioration du personnel de l'enseignement supérieur (CAPES), « Coordination for the Improvement of Higher Education Personnel (CAPES) », *http://www.iie.org/Programs/CAPES*, et CNPq, « Programas Institucionais de Iniciação Científica e Tecnológica », *http://www.cnpq.br/web/guest/piict*.

74. « Cyber Security », The Hague Security Delta, *https://www.thehaguesecuritydelta.com/cyber-security*.

75. Zach Cutler, « 5 Growing Cyber Security Epicenters Around the World », *Entre- preneur*, 3 septembre 2015, *http://www.entrepreneur.com/article/250024*.

76. Commission européenne, « About TTIP », *Trade, http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/*.

77. « Welcome to the U.S.-EU Safe Harbor », *http://www.export.gov/safeharbor/eu/eg_main_018365.asp*.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

78. Cour de Justice de l'Union européenne, « The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid », *Communiqué de presse* 117/15 (6 October 2015), *http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf*.

79. Chambre de commerce américaine au sein de l'Union européenne, « EU Courts of Justice's decision in the Schrems case could disrupt transatlantic business, hurt the EU economy and jeapordise a Digital Single Market », Communiqué de presse, 6 octobre 2015, *http://www.amchameu.eu/sites/default/files/press_releases/press_-_ecj_decision_on_schrems_will_disrupt_transatlantic_business.pdf*.

80. Hathaway, « Connected Choices: How the Internet Is Challenging Sovereign Decisions », 302 et Arun Mohan Sukmar, « The New Great Game in Asia », *The Hindu*, 25 août 2015, obtenu le 16 septembre 2015, *http://www.thehindu.com/opinion/op-ed/arun-mohan-sukumar-column-the-new-great-game-in-asia/article7575755.ece*.

81. « Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies », dernière mise à jour le 16 septembre 2015, *http://www.wassenaar.org/index.html*.

82. Nations Unies, « *Report of the Group of Government Experts On Development in the Field of Information and Telecommunications In the Context of International Security* », A/65/201 et A/68/98 (26 juin 2015).

83. Bureau du Secrétaire de presse de la Maison Blanche, « FACT SHEET: President Xi Jinping's State Visit to the United States », 25 septembre 2015, *https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states*.

84. Université de Toronto, « VII: BRICS Summit 2015 Ufa Declaration », *BRICS Information Centre*, 9 juillet 2015, *http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html*.

85. Assemblée générale des Nations Unies, « Letter dated 9 January 2015 from Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General », Projets dans le domaine de l'information et des communications dans le contexte de la sécurité internationale, A/69/723 (13 janvier 2015), *http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement*.

86. Melissa Hathaway, « Discussion Paper for the Global Commission of Internet Governance », (document présenté à Stockholm en Suède le 27 mai 2014).

87. Banque de développement interaméricaine, « IDB and OAS join efforts to promote better cybersecurity policies in Latin America and the Caribbean », 22 octobre 2014, *http://www.iadb.org/en/news/news-releases/2014-10-22/cybersecurity-workshop-for-latin-america,10957.html*.

88. Dusan Navratil, Directeur, Autorité de la sécurité nationale tchèque et Robert Kahofer, Assistant spécialisé, « Cyber Czech 2015 - National Technical Cyber Security Exercise », (entretien réalisé par Melissa Hathaway à Washington DC en octobre 2015) et Rueuven Azar, Assistant du Chef de mission et Dr. Eviatar Matania, Chef du cyberbureau national (entretien réalisé par Melissa Hathaway à Rockville, MD, le 2 juin 2015).

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

89. Craig L. Hall, Consulat général américain, Kolkata, Inde, (entretien réalisé par Melissa Hathaway à Kolkata en Inde, le 23 septembre 2015).

90. Les cyberconflits sont différents des cyberguerres ou des batailles contre la cybercriminalité. Ces dernières sont des batailles purement technologiques qui pourraient, en principe, être intégralement menées au sein d'un réseau. Elles font généralement partie intégrante des cyberconflits ou cyberguerres. « Les cyberconflits sont des conflits agressifs et perturbateurs importants sur le plan national, pour lesquels des événements typiques déterminant les résultats n'auraient pas pu avoir lieu sans la mise en place de systèmes « cybernétiques » (c'est-à-dire des technologies en réseau) pendant les moments critiques de ces événements », Chris Demchak, « Resilience, Disruption, and a 'Cyber Westphalia' : Options for National Security in a Cybered Conflict World », dans « Securing Cyberspace: A New Domain for National Security », édité par Nicholas Burns et Jonathon Price, (Washington, DC : The Aspen Institute, 2012).

91. Christopher Bronk, « The Cyber Attack on Saudi Aramco », Survival 55 (Avril-mai 2013) 81-96.

92. Melissa Hathaway et John Stuart, « Cyber IV Feature: Taking Control of our Cyber Future », *Georgetown Journal of International Affairs* (25 juillet 2014).

93. Robert M. Lee, Michael J. Assante, et Tim Conway, « German Steel Mill Cyber Attack », *Industrial Control Systems* (30 décembre 2014).

94. The Reality of the Sony Pictures Breach », *TrendMicro*, 22 décembre 2014, *http://blog.trendmicro.com/reality-sony-pictures-breach/*, Sean Fitz-Gerald, « Everything That's Happened in the Sony Leak Scandal », *Vulture*, 22 décembre 2014, *http://www.vulture.com/2014/12/everything-sony-leaks-scandal.html#*, et « Sony Breach May Have Exposed Employee Healthcare, Salary Data », *Krebson Security*, 2 décembre 2014, *http://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/*.

95. Jennifer Valentino-Devries et Danny Yadron, « Cataloging the World's Cy- berforces », The Wall Street Journal, 11 octobre 2015, *http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710* et Assemblée générale des Nations Unies : « *Developments in the Field of Information and Tele- communications in the context of International Security: Report to the Secretary General* », A/70/172 (22 juillet 2015), *http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172*.

96. James Lewis et Katrina Timlin, « Cy- bersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization », *UNIDIR Resource and Center for Strategic and International Studies* (2011): 3.

97. Ministère de la défense, « The Department of Defense Cyber Strategy », (Avril 2015): 7-8.

98. Président de la Fédération russe, « Military Doctrine of the Russian Federation », *Gouvernement russe* (2014) traduit par Thomas Moore, *https://www.scribd.com/doc/251695098/Russia-s-2014-Military-Doctrine*.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

99. Ministère de la défense de la Fédération russe, « Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the In- formation Space », (2011) traduit par le département d'État américain.

100. « The new doctrine of information secu- rity pointed out the danger of destabi- lization via the Internet », Actualités russes, 10 septembre 2015, *http://en.news-4-u.ru/the-new-doctrine-of-information-security-pointed-out-the-danger-of-destabilization-via-the-internet.html*.

101. Le Ministère de la défense brésilien a également récemment demandé à l'État-major conjoint des Forces armées (EMCFA) d'améliorer son système de cyberdéfense national en créant une unité de contrôle et de défense cybernétiques à trois services (ComDCiber). Bien que la ComDCiber inclue trois services, l'Armée assumera le rôle de chef de file. La ComDCiber sera basée sur l'ancien NU CDCiber brésilien (Cyber Defense Center Nucleus) situé à Brasilia. Voir eeInigo Guevara : « Brazil to stand up Cyber Defence Command », IHS Jane's Defence Weekly, 4 novembre 2014 et Diego Rafael Canabarro et Thiago Borne : « Brazil and the Fog of (Cyber) War », Centre national pour la gouvernance numérique (2013): 5. Concernant les capacités de lutte contre la cybercriminalité coréenne, consulter : République de Corée : « Defense White Paper » (2014), 57, *http://www.mnd.go.kr/user/mnd_eng/upload/pblictn/PBLICTNEBOOK_20150161156164570.pdf*.

102. Zachary Keck, « South Korea Seeks Offensive Cyber Capabilities », *The Diplomat*, 11 octobre 2014, *http://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites/*.

103. Pour un aperçu de la cyberstratégie chinoise, consulter : Amy Chang : « Warring States », *The Center for New American Security*, (Décembre 2014).

104. Bureau d'information de l'État, « White Paper: The Diversified Employment of China's Armed Forces », Avril 2013, *http://eng.mod.gov.cn/Database/WhitePapers/* et Xi Jinping, Central Military Commission, « Opinion on Further Strengthening Military Information Security Work », traduction partielle effectuée par Amy Chang, « Warring States », The Center for New American Security, (Décembre 2014): 20.

105. Directeurs généraux du Conseil nordique, « Icelandic Cyber Responsibilities », (réunion entre Melissa Hathaway et les directeurs généraux et délégations respectives du Conseil nordique qui sont chargés de la gestion des équipes nationales de réponse aux urgences informatiques, Stockholm, Suède, le 19 novembre 2014).

106. Ministre de l'intérieur, « Icelandic National Cyber Security Strategy 2015-2026: Plan of Action », Ministre de l'intérieur islandais (Juin 2015), *http://eng.innanrikisraduneyti.is/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf*.

107. Yaakov Katz, « Security and Defense », The Jerusalem Post, 8 octobre 2010 dans : James Lewis et Katrina Timlin : « Cyber-security and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization », *UNIDIR Resource and Center for Strategic and International Studies* (2011), 14 et « Eye on tech exports, Israel launches cyber command », Reuters, 18 mai 2011, *http://www.reuters.com/article/2011/05/18/us-israel-security-cyber-idUSTRE74H27H20110518*.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

108. Mitch Ginsburg, « Army to establish unified cyber corps », The Times of Israel, 16 juin 2015.

109. Michael Herzog, « New IDF Strategy Goes Public », The Washington Institute: Policy Watch 2479 (28 août 2015), *http://www.washingtoninstitute.org/policy-analysis/view/new-idf-strategy-goes-public*.

© 2015 Indice de préparation à la lutte contre la cybercriminalité – Version 2.0, tous droits réservés

À PROPOS DES AUTEURS

Melissa Hathaway est spécialisée dans les domaines de la cybersécurité et des politiques liées au cyberespace. Elle est agrégée supérieure et membre du conseil d'administration du Potomac Institute for Policy Studies, puis conseillère principale du Belfer Center for Science and International Affairs de la Harvard Kennedy School. Elle est également membre honoraire du Centre for International Governance Innovation dont le siège est au Canada, et a été nommée membre de la Global Commission for Internet Governance (une commission créée par Bildt). 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. Elle a élaboré une méthodologie unique de mesure et d'évaluation des niveaux de capacité à lutter contre certains risques liés à la cybersécurité, mieux connue sous le nom d' « Indice de préparation à la lutte contre la cybercriminalité ». Elle publie régulièrement des articles sur des thèmes liés à la cybersécurité qui affectent les différents pays et entreprises. La plupart de ses articles peuvent être consultés sur le site suivant : *http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html*.

Chris Demchak est spécialisée dans le projet portant sur l'Indice de préparation à la lutte contre la cybercriminalité élaboré par le Potomac Institute for Policy Studies. Ses domaines de recherche incluent la résilience numérique, les cyberconflits, ainsi que les structures et les risques liés au cyberespace. Elle a élaboré un modèle d'organisation numérique appelé « Atrium » qui aide les grandes entreprises à répondre et à s'adapter aux surprises qui peuvent apparaître au sein de leurs systèmes. Elle est par ailleurs l'auteure des ouvrages intitulés « Wars of Disruption » et « Resilience: Cybered Conflict, Power and National Security ».

Jason Kerben est spécialisé dans le projet portant sur l'Indice de préparation à la lutte contre la cybercriminalité élaboré par le Potomac Institute for Policy Studies. Il est également conseiller principal auprès de plusieurs ministères et organismes, sur des thèmes liés à la sécurité de l'information et à la cybersécurité. Ses travaux sont particulièrement axés sur les régimes juridiques et réglementaires qui ont un impact sur la mission d'une organisation. Il développe des méthodologies et des approches permettant d'évaluer et de gérer les risques liés à la cybersécurité ; en outre, et il fournit des conseils sur une multitude d'activités spécifiquement liées à la cybersécurité, notamment les principes internationaux qui régissent les technologies de l'information et des communications, la gestion des identités et des accès, le diagnostic continu, l'atténuation des risques et la cyberassurance.

Jennifer McArdle est membre du Center for Revolutionary Scientific Thought au sein du Potomac Institute for Policy Studies. Ses travaux de recherche universitaire sont axés sur la cyberguerre, la guerre de l'information et la géopolitique asiatique. Elle est actuellement doctorante au sein du département de l'étude des guerres (War Studies) du King's College de Londres.

Francesca Spidalieri est spécialisée dans le projet lié à l'Indice de préparation à la lutte contre la cybercriminalité élaboré par le Potomac Institute for Policy Studies. Elle est également agrégée supérieure en « cyberleadership » au sein du Pell Center de la Salve Regina University. Ses publications et travaux de recherche universitaire sont axés sur le développement d'un cyberleadership, la gestion des cyber-risques, l'éducation et la sensibilisation aux questions cybernétiques et la création d'un personnel spécialisé dans la cybersécurité. Elle a récemment publié un rapport intitulé « State of the States on Cybersecurity » (État des lieux des pays en matière de cybersécurité) qui applique, au niveau des états américains, le document « Indice de préparation à la lutte contre la cybercriminalité – Version 1.0 ».

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203, États-Unis
www.potomacinstitute.org