Union internationale des télécommunications

QUESTION 22/1

Rapport final

UIT-D COMMISSION D'ETUDES 1 4e PERIODE D'ETUDES (2006-2010)

QUESTION 22/1:

Sécurisation des réseaux d'information et de communication: meilleures pratiques pour créer une culture de la cybersécurité

LES COMMISSIONS D'ÉTUDES DE L'UIT-D

Aux termes de la Résolution 2 (Doha, 2006), la CMDT-06 a maintenu l'existence de deux commissions d'études et a déterminé les Questions qu'elles devaient étudier. Les méthodes de travail que doivent suivre les commissions d'études sont décrites dans la Résolution 1 (Doha, 2006) adoptée par la CMDT-06. Pour la période 2006-2010, la Commission d'études 1 a été chargée de l'étude de neuf Questions dans le domaine des stratégies et politiques de développement des télécommunications. La Commission d'études 2 a été chargée de l'étude de dix Questions dans le domaine du développement et de la gestion des services et des réseaux de télécommunication et des applications des TIC.

Pour tout renseignement

Veuillez contacter:

M. Souheil MARINE/Mme Christine SUND
Bureau de développement des télécommunications (BDT)
UIT
Place des Nations
CH-1211 GENÈVE 20
Suisse
Téléphone: +41 22 730 5323/ 5203
Fax: +41 22 730 5484
E-mail: souheil.marine@itu.int
christine.sund@itu.int

Pour commander les publications de l'UIT

Les commandes ne sont pas acceptées par téléphone. Veuillez les envoyer par téléfax ou par e-mail.

UIT
Service des ventes
Place des Nations
CH-1211 GENÈVE 20
Suisse
Fax: +41 22 730 5194
E-mail: sales@itu.int

La Librairie électronique de l'UIT: www.itu.int/publications

UIT-D COMISSION D'ÉTUDES 1 4e PÉRIODE D'ÉTUDES (2006-2010)

QUESTION 22-1:

Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité

TABLE DES MATIERES

QUESTION 22-1

Introduction

Le présent rapport donne aux administrations nationales un aperçu des éléments de base nécessaires pour aborder de la cybersécurité au niveau national et organiser la manière d'envisager la cybersécurité dans les pays[1]. Dans la mesure où les capacités nationales existantes varient et où les menaces ne cessent d'évoluer, le rapport ne constitue pas une prescription pour la sécurisation du cyberespace. En revanche, ce cadre décrit une approche souple qu'une administration nationale peut utiliser pour passer en revue et améliorer ses institutions, ses politiques générales et ses relations existantes en matière de cybersécurité. Bien que le présent rapport mette l'accent sur la cybersécurité, il convient de noter que la protection du réseau proprement dit constitue une priorité tout aussi importante. Nous soulignons également que les bonnes pratiques en matière de cybersécurité doivent protéger et respecter les dispositions relatives à la vie privée et à la liberté d'expression, telles qu'elles figurent dans les parties pertinentes de la Déclaration universelle des droits de l'homme et de la Déclaration de principe de Genève.[2]

Les principes essentiels abordés dans le présent rapport sont les suivants:

- Elaborer une stratégie nationale en matière de cybersécurité.
- Etablir une collaboration au niveau national entre les pouvoirs publics et le secteur privé.
- Prévenir la cybercriminalité.
- Créer des moyens nationaux de gestion des incidents.
- Promouvoir une culture nationale de la cybersécurité.

Chacun de ces principes devrait faire partie d'une approche nationale globale de la cybersécurité. L'ordre d'apparition des principes n'indique aucune prévalence d'un élément sur un autre. D'autres principes pourraient être retenus en fonction des spécificités de chaque pays.

Pour les besoins du présent rapport, on entend par ***cybersécurité,*** au sens de la Recommandation UIT-T X.1205, l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, mesures, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les ressources des organisations et des utilisateurs. Ces ressources comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication ainsi que la totalité des informations transmises ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des ressources des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants:

- Disponibilité.
- Intégrité, qui peut englober l'authenticité et la non-répudiation.
- Confidentialité.

---

[1] Les lecteurs intéressés sont invités à prendre connaissance des résultats obtenus grâce aux normes ISO 27001 et 27003.

[2] Voir l'Agenda de Tunis pour la société de l'information du SMSI, paragraphe 42.

Il est important de comprendre la relation qui existe entre la cybersécurité, les infrastructures essentielles (CI), les infrastructures essentielles de l'information (CII), la protection des infrastructures essentielles de l'information (CIIP) et enfin, les infrastructures non essentielles. Ces relations sont illustrées sur la Figure 1.

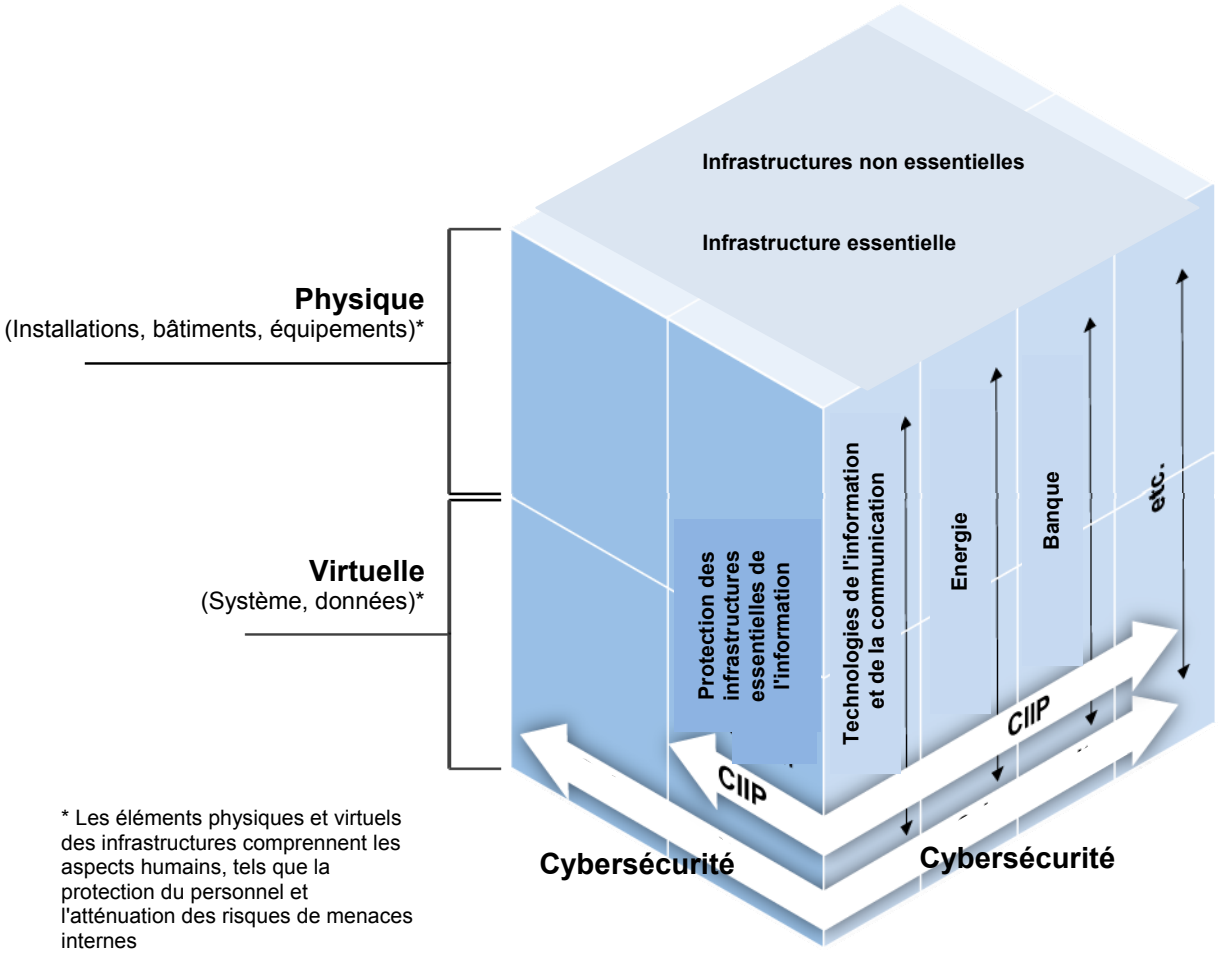
Si les définitions peuvent varier légèrement, on considère en général que les ***infrastructures essentielles*** (CI) sont les principaux systèmes, services et fonctions dont l'interruption ou la destruction aurait des effets dévastateurs sur la santé et la sécurité publiques, le commerce et la sécurité nationale ou toute combinaison de ces aspects. Les infrastructures essentielles comprennent à la fois des éléments concrets (installations et bâtiments) et des éléments virtuels (systèmes et données) (voir la Figure 1). Le caractère "essentiel" peut varier d'un pays à l'autre, mais on considère en général que ce type d'infrastructure pourrait notamment comporter des éléments appartenant aux secteurs suivants: technologies de l'information et de la communication (TIC), énergie, banques, transports, santé publique, agriculture et alimentation, eau, produits chimiques, transports maritimes et services publics indispensables. A chaque étape de leur développement, les pays doivent planifier et élaborer des politiques pour protéger ce qui, à leur avis, constitue leurs IC (c'est-à-dire les infrastructures essentielles qui incluent la protection physique et virtuelle), afin d'offrir une garantie raisonnable sur le plan de la souplesse et de la sécurité pour mener à bien les missions du pays et assurer stabilité économique.

Chacun de ces secteurs économiques dispose de ses propres ressources matérielles: bâtiments des banques, centrales électriques, trains, hôpitaux et bureaux de l'Etat. Toutefois, ces secteurs essentiels de l'économie d'un pays dépendent tous des technologies de l'information et de la communication. D'une manière générale, ces secteurs et leurs ressources matérielles dépendent aujourd'hui du fonctionnement fiable de ces ***infrastructures essentielles de l'information*** (CII) pour la fourniture de leurs services et le déploiement de leurs activités. Par conséquent, une interruption majeure de ces infrastructures pourrait avoir des effets immédiats et dévastateurs qui vont bien au-delà du secteur des TIC et nuisent ainsi à la capacité d'un pays d'atteindre ses objectifs fondamentaux dans de nombreux secteurs. Un programme de ***protection des infrastructures essentielles de l'information*** (CIIP) protège la composante virtuelle des CII.

Comme indiqué dans la Figure 1, le CIIP est un sous-ensemble des TIC et de la cybersécurité. La cybersécurité assure une protection contre tous les types de cyberincidents, en renforçant la sécurité des infrastructures essentielles de l'information dont dépendent les secteurs essentiels et en sécurisant les réseaux et les services qui répondent aux besoins quotidiens des utilisateurs. Les cyberincidents peuvent avoir des incidences aussi bien sur les infrastructures essentielles que sur les infrastructures non essentielles de l'information et donner lieu à de nombreux types d'activités malveillantes: utilisation de botnets pour se livrer à des attaques par déni de service et envoyer des spams et des maliciels (par exemple, virus et vers informatiques) qui nuisent au fonctionnement des réseaux. De plus, les cyberincidents peuvent englober des activités illicites comme le phishing (hameçonnage) et le pharming (détournement vers des sites frauduleux) ainsi que l'usurpation d'identité. Les cybermenaces sont toujours plus nombreuses à mesure que les outils et les méthodologies utilisés se généralisent et que les capacités techniques et le degré de perfectionnement des cybercriminels se développent. Quel que soit leur stade de développement, tous les pays ont connu ces cyberincidents.

Une approche nationale de la cybersécurité suppose une prise de conscience des risques existants, la création de structures nationales pour aborder la cybersécurité et l'établissement des relations nécessaires qui peuvent être utilisées lorsque des cyberincidents se produisent. L'évaluation des risques, la mise en place de mesures d'intervention d'urgence et la gestion des conséquences font aussi partie d'un programme national de cybersécurité. L'existence d'un programme national de cybersécurité bien conçu contribuera à protéger l'économie d'un pays contre toute désorganisation, en assurant la planification entre les secteurs, en protégeant les informations stockées dans les systèmes informatiques, en préservant la confiance du public, en assurant la sécurité nationale et, enfin, en garantissant la santé et la sécurité publiques.

Figure 1: Relations entre la cybersécurité et la protection des infrastructures essentielles de l'information



Le renforcement de la cybersécurité ne saurait être assuré uniquement dans le cadre de stratégies nationales, même s'il doit y occuper une place très importante. Il doit également être complété par des stratégies régionales et internationales, comme cela est préconisé dans les documents pertinents des résultats du SMSI élaborés lors des phases de 2003 et 2005 ainsi que dans la grande orientation C5, notamment les numéros 35 et 36 de la Déclaration de principes de Genève et le N° 39 de l'Agenda de Tunis. Il doit également être réalisé dans le cadre de la mise en œuvre des résultats du Sommet mondial sur la société de l'information par le biais des résolutions, des mesures et des initiatives en la matière adoptées par l'UIT, notamment:

a) Objectif 4 de la Résolution 71 (Rév. Antalya 2006) de la Conférence de plénipotentiaires "Plan stratégique de l'Union pour 2008-2011".

b) Résolution 130 (Rév. Antalya 2006) de la Conférence de plénipotentiaires "Renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication".

c) Les sections pertinentes du Plan d'action de Doha de la CMDT-06, y compris le Programme 3 relatif aux cyberstrategies et aux applications TIC qui identifient la cybersécurité comme une priorité pour le BDT, avec des activités définies et en particulier l'adoption de la Résolution 45 (Doha, 2006)

intitulée "Mécanismes propres à améliorer la coopération en matière de cybersécurité, y compris la lutte contre le spam". La Résolution 45 chargeait le Directeur du BDT d'organiser des réunions pour débattre des moyens d'améliorer la cybersécurité, notamment dans le cadre d'un Mémorandum d'accord conclu entre les Etats Membres intéressés ayant pour objet d'améliorer la cybersécurité et de combattre le spam, et de rendre compte des résultats de ces réunions à la Conférence de plénipotentiaires de 2006. Le rapport du BDT à la Conférence de plénipotentiaires de 2006 est disponible à l'adresse suivante: www.itu.int/md/S06-PP-C-0024/en.[3]

d) Les travaux approfondis réalisés par la Commission d'études 17 de l'UIT-T sur la cybersécurité et les activités complémentaires menées par la Commission d'études 13.

e) La Résolution 58 adoptée par l'AMNT (Johannesburg, 2008) visant à encourager la création d'équipes d'intervention en cas d'incident informatique (CIRT) à l'échelle nationale, en particulier dans les pays en développement, qui a reconnu les travaux effectués au titre de cette Question 22.1 par le Secteur de l'UIT-D.

f) Le Rapport du Président du Groupe d'experts de haut niveau(HLEG) sur le Programme mondial cybersécurité lancé par le Secrétaire général le 17 mai 2007 récapitule les propositions formulées par des experts au sujet des sept objectifs stratégiques principaux de ce Programme, l'accent étant mis sur les recommandations applicables aux cinq domaines de travail suivants:
   – Cadre juridique
   – Mesures techniques et relatives aux procédures
   – Structures organisationnelles
   – Renforcement des capacités
   – Coopération internationale

   Parmi ces domaines de travail, des "mesures juridiques" visent à étudier les problèmes législatifs posés par les activités criminelles sur les réseaux TIC selon une approche compatible au niveau international. Les "mesures techniques et de procédures" traitent des principales mesures propres à encourager l'adoption de méthodes visant à améliorer la sécurité et la gestion des risques au sein du cyberespace, notamment des systèmes d'accréditation, des protocoles et des normes. Les "structures organisationnelles" portent sur la prévention, la détection, l'intervention et la gestion de crise des cyberattaques, notamment la protection des systèmes d'infrastructures d'informations essentielles. Le "renforcement des capacités" vise à élaborer des stratégies relatives aux mécanismes de renforcement des capacités pour favoriser la sensibilisation, transférer les connaissances et encourager la cybersécurité dans le cadre de programmes politiques nationaux. Enfin, la "coopération internationale" est axée sur le dialogue et la coordination dans la gestion des cybermenaces.[4, 5]

g) Le projet d'Avis 4 adopté récemment par le Forum mondial des politiques de télécommunication (FMPT) de 2009 sur les "stratégies de collaboration pour instaurer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication"[6], en particulier les parties *invite l'UIT* et *invite les Etats Membres*.

h) Les activités au titre du Programme 3 (cyberapplications) menées par le BDT: assistance directe apportée aux Etats Membres des pays en développement, projets et activités de renforcement des capacités, kit pratique de l'UIT pour l'autoévaluation relative à la cybersécurité/CIIP au niveau

---

[3] Compte tenu de l'expérience qu'ils ont acquise au cours des quatre dernières années, les Etats arabes sont convaincus qu'un mémorandum d'accord entre les Etats Membres pour améliorer la cybersécurité et lutter contre le spam constitue la meilleure solution pour répondre aux besoins mondiaux ou régionaux.

[4] Des experts des Etats arabes ont appuyé toutes les recommandations formulées dans le Rapport du Président du Groupe HLEG.

[5] Le Rapport du Président du Groupe HLEG est disponible à l'adresse suivante: www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf

[6] Le projet d'Avis 4 du FMPT est disponible dans sa totalité à l'adresse suivante: www.itu.int/osg/csd/wtpf/wtpf2009/documents/opinion4.pdf

national, kit pratique de l'UIT pour atténuer les effets des botnets et kit pratique pour la création de CIRT (équipes d'intervention en cas d'incident informatique) à l'échelle nationale.

i) L'initiative de protection des enfants en ligne (COP) a été lancée en novembre 2008 sous la forme d'un réseau international de collaboration, dont le but est de promouvoir la protection des enfants et des jeunes en ligne dans le monde entier en fournissant des directives sur la sécurité du comportement en ligne, conjointement avec d'autres organismes des Nations Unies et d'autres partenaires. Les principaux objectifs de cette initiative sont les suivants: 1) identifier les principaux risques et dangers du monde virtuel pour les enfants et les jeunes; 2) sensibiliser l'opinion aux risques et aux problèmes par différents moyens; 3) élaborer des outils pratiques destinés à aider les gouvernements, les organisations et les éducateurs à minimiser les risques; et 4) communiquer les connaissances et les données d'expérience, tout en facilitant l'établissement de partenariats stratégiques au niveau international, afin de définir et de mettre en œuvre des initiatives concrètes.

j) La collaboration établie entre l'UIT et l'initiative IMPACT (Partenariat multilatéral international contre les cybermenaces) dans le cadre du Programme mondial cybersécurité de l'Union vise à rassembler les principales parties prenantes et principaux partenaires issus des gouvernements, du secteur privé et des milieux universitaires, afin d'apporter aux Etats Membres de l'UIT, les connaissances spécialisées, les moyens et les ressources nécessaires pour lutter efficacement contre les cybermenaces. Les principaux objectifs de la collaboration UIT-IMPACT sont les suivants: 1) élaborer un cadre mondial pour la veille, l'alerte et l'intervention en cas d'incident; 2) établir des structures organisationnelles et des politiques appropriées aux niveaux national et régional, par exemple des équipes CIRT; 3) faciliter le renforcement des capacités humaines et institutionnelles dans les différents secteurs; et 4) favoriser la coopération internationale entre plusieurs parties prenantes à l'échelle mondiale.

PARTIE I

Elaborer et obtenir un accord concernant une stratégie nationale de la cybersécurité

L'élaboration et la mise en œuvre d'un plan national en matière de cybersécurité exigent une stratégie globale qui consiste à recenser les pratiques nationales actuelles en vue d'en évaluer la pertinence et à tenir compte du rôle que joue l'ensemble des partenaires (pouvoirs publics, secteur privé et particuliers) dans le processus.

Pour des raisons de sécurité nationale et de bien-être économique, les pouvoirs publics ont besoin de faciliter, de promouvoir et d'assurer la protection de leurs infrastructures essentielles de l'information. Aujourd'hui, les infrastructures de l'information traversent les secteurs industriels des pays et ne connaissent pas de frontières. L'ubiquité de ces infrastructures essentielles de l'information offre des possibilités et des avantages économiques considérables qui s'accompagnent de relations d'interdépendance et de risques coûteux. Une étude réalisée à la demande du Bureau de développement des télécommunications (BDT) de l'UIT résume ces coûts de la façon suivante[7]:

> Les dépenses et les recettes de tous les partenaires de la chaîne de services d'information, tels que les fournisseurs de logiciels, les opérateurs de réseaux, les fournisseurs de services Internet et les utilisateurs, subissent les conséquences des logiciels malveillants et du spam. Ces conséquences sont diverses: coût des mesures préventives, coût des mesures correctives, coûts directs de la largeur de bande et des équipements et coûts d'opportunité de l'encombrement des réseaux. Toutefois, la situation se complique du fait que le spam et les logiciels malveillants créent aussi de nouvelles sources de recettes, légitimes ou non. Ils sont aussi à l'origine de modèles économiques légitimes (produits antivirus et antispam, infrastructures et largeur de bande associées) ou délictueux (location de botnets, commissions perçues sur les ventes qu'entraîne l'envoi de spam, campagnes de spam boursier, etc.). Par conséquent, les partenaires se retrouvent dans des situations ambivalentes et parfois conflictuelles, ce qui rend plus difficile de réagir de manière cohérente.

La politique nationale de la plupart des pays consiste depuis longtemps à traiter le réseau téléphonique public commuté (RTPC) comme une infrastructure essentielle et à le protéger en conséquence. Dans de nombreux pays, les entreprises commerciales possèdent des parties importantes de cette infrastructure du RTPC et ont participé à cet effort en collaborant entre elles ainsi qu'avec les pouvoirs publics. La progression rapide des TIC numériques dans les réseaux de télécommunication filaires ou hertziens interconnectés a cependant profondément modifié la nature de la sécurité des réseaux et les exigences associées, tant et si bien que les politiques et les procédures de sécurité basées sur le RTPC traditionnel sont peut-être devenues insuffisantes pour répondre aux nouvelles exigences de sécurité.

Les changements induits par les TIC exigent que les pouvoirs publics, les entreprises, d'autres organisations ainsi que les utilisateurs individuels qui conçoivent, possèdent, fournissent, gèrent, entretiennent et utilisent des systèmes et réseaux d'information coopèrent davantage. Cependant, alors que les pouvoirs publics continuent souvent à prendre l'initiative en élaborant des politiques publiques liées à la sécurité des réseaux, il est vital de s'assurer que d'autres parties prenantes, dont les opérateurs et constructeurs d'infrastructures, sont intégrées dans le processus global de planification et d'élaboration des politiques. C'est en œuvrant ensemble que les pouvoirs publics et le secteur privé pourront tirer efficacement parti de leurs compétences respectives et gérer les risques inhérents aux CII. Cette intégration engendre une plus grande confiance et permet l'élaboration et l'application optimales des politiques et des technologies. Au niveau international, la protection des infrastructures essentielles de l'information et le renforcement de la cybersécurité nécessitent la coopération et la coordination entre les pays et avec les partenaires internationaux.

---

[7] Voir le projet d'étude "Aspects financiers de la sécurité des réseaux: logiciels malveillants et spam", Document UIT-D 1/144 (6 mai 2008).

I.A Aperçu des objectifs de cette partie

I.A.1 Susciter une sensibilisation aux questions de cybersécurité au niveau politique national, et à la nécessité d'agir au niveau national et d'instaurer une coopération internationale.

I.A.2 Mettre au point une stratégie nationale visant à renforcer la cybersécurité afin de réduire les risques et les effets des dysfonctionnements du cyberespace ainsi que d'ordre physique.

I.A.3 Participer aux efforts internationaux visant à promouvoir les activités nationales liées aux incidents (prévention, préparation, intervention et retour à la normale).

I.B Mesures spécifiques pour atteindre ces objectifs

Les objectifs susmentionnés sont communs à tous les pays; cependant, les mesures spécifiques prises pour atteindre ces objectifs varieront selon les besoins et les conditions propres à chaque pays. Dans de nombreux pays, les pouvoirs publics prendront ces mesures.

I.B.1 Persuader les dirigeants du gouvernement de la nécessité d'agir au niveau national pour faire face aux menaces et aux vulnérabilités concernant les infrastructures électroniques nationales via des discussions au niveau politique.

1. Un pays qui cherche à améliorer la cybersécurité et à sécuriser ses infrastructures essentielles de l'information doit, dans un premier temps, instaurer la cybersécurité en tant que politique nationale. D'une manière générale, une déclaration concernant la politique adoptée au niveau national en matière de cybersécurité: (1) reconnaît l'importance des CII pour le pays; (2) identifie les risques encourus (habituellement, une approche tous risques[8]); (3) fixe l'objectif à atteindre en ce qui concerne la politique de cybersécurité; et (4) indique dans ses grandes lignes les moyens de la mettre en œuvre, y compris par une collaboration avec les partenaires appropriés.

   Une fois que la politique globale de la cybersécurité est clairement définie, elle peut être complétée par une stratégie nationale qui délimite les rôles et les responsabilités, recense les priorités et fixe le calendrier ainsi que les mesures à prendre pour la mise en œuvre. De plus, selon la politique et la stratégie adoptées, il peut aussi être décidé d'inscrire les efforts à déployer au niveau national dans le cadre d'autres activités internationales en matière de cybersécurité. Pour parvenir à une politique globale de la cybersécurité, il peut s'avérer nécessaire de mieux faire connaître ces questions aux principaux décideurs. Ceux-ci doivent comprendre qu'il faut peut-être du temps avant d'atteindre les objectifs de cybersécurité convenus.

2. Un cadre de cybersécurité national ne doit pas se composer de politiques immuables. Au contraire, il faut que le cadre et les politiques soient souples et permettent de répondre à l'environnement dynamique des risques. Ce cadre devrait fixer des objectifs en matière de politique générale. En établissant des objectifs clairs, les organismes publics et les entités non gouvernementales peuvent œuvrer ensemble pour atteindre les objectifs énoncés de la façon la plus efficace qui soit.

3. Cette politique nationale devrait être élaborée en coopération, via des consultations entre des représentants de tous les groupes compétents de parties prenantes, y compris les organismes publics, le secteur privé, les milieux universitaires et les associations intéressées. Cette politique devrait être promulguée au niveau national, de préférence par le chef du gouvernement.

---

[8] Une approche *tous risques* ou *multirisques* de la gestion des risques tient compte de tous les risques potentiels d'ordre naturel ou technologique; il s'agit des situations d'urgence et des catastrophes aussi bien naturelles qu'artificielles (de type accidentel ou volontaire).

I.B.2 Identifier une personne et une institution qui seront responsables de l'ensemble de l'effort national; déterminer où, dans l'administration publique, devrait être établi un centre d'alerte et de réaction aux attaques informatiques (CSIRT, computer security incident response team[9]), doté d'une responsabilité nationale[10]; et identifier les institutions responsables de chaque aspect de la stratégie nationale.

1. Pour lancer une initiative de cybersécurité, il faut, dans la phase initiale, identifier la personne qui dirigera l'effort national de cybersécurité, c'est-à-dire une personne à un niveau politique du gouvernement qui comprenne les questions de cybersécurité et qui puisse diriger et coordonner les efforts des institutions gouvernementales et interagir efficacement avec le secteur privé. Idéalement parlant, cette personne devrait avoir une stature politique et avoir accès au chef du gouvernement. Une telle autorité de haut niveau est nécessaire pour garantir la coordination entre des entités qui doivent interagir. A la longue, cet effort de coordination constituera une base institutionnelle pour les dirigeants et les organisations techniques du pays dans le domaine de la cybersécurité.

2. Une fois que le pays aura lancé une initiative de cybersécurité, la personne ou l'institution qui en est à l'origine n'aura peut-être plus besoin de jouer ce rôle.

3. D'autres institutions responsables du développement et de la mise en œuvre des différentes parties d'une stratégie nationale de sécurité doivent être identifiées.

I.B.3 Identifier les experts et décideurs compétents au sein de l'administration publique et du secteur privé et définir leur rôle.

1. Une action nationale efficace nécessite que l'on inculque une "culture de la cybersécurité" parmi toutes les parties prenantes. Toutes les personnes et les institutions, au sein de l'administration publique comme en dehors, qui développent, possèdent, fournissent, gèrent, entretiennent et utilisent des systèmes et réseaux d'information doivent comprendre le rôle qu'elles doivent jouer ainsi que les mesures qui doivent être prises. Les principaux décideurs et les dirigeants du secteur privé doivent établir des buts et des priorités au sein de leurs institutions. Des experts techniques de haut vol doivent donner des lignes directrices et des cadres d'action.

I.B.4 Identifier des arrangements coopératifs pour et entre toutes les parties prenantes.

1. Les pouvoirs publics nationaux devraient encourager les arrangements collaboratifs, officiels ou officieux, qui permettent et favorisent la communication et le partage d'informations entre les secteurs privé et public. La cybersécurité sera mise en œuvre au niveau technique ou opérationnel par un vaste ensemble d'institutions publiques et autres. Ces efforts doivent également être coordonnés et comprendre des mécanismes de partage de l'information.

I.B.5 Instaurer des mécanismes de coopération entre secteur public et secteur privé au niveau national.

1. Le développement des orientations politiques ainsi que l'élaboration et la mise en œuvre du plan national doivent se faire selon des processus ouverts et transparents, et prendre en compte les opinions et les intérêts de toutes les parties prenantes.

I.B.6 Identifier des homologues internationaux et favoriser les efforts internationaux visant à traiter des questions de cybersécurité, y compris le partage de l'information et les efforts d'assistance, compte tenu des résultats du projet de mise en œuvre de la Résolution 45 de la CMDT-06.

1. L'effort d'amélioration de la cybersécurité nationale sera facilité par la participation à des forums régionaux ou internationaux, souvent sous la forme de conférences et d'ateliers, qui peuvent être

---

[9] Un CSIRT est une équipe d'experts en sécurité informatique ayant pour mission principale de répondre aux incidents liés à la sécurité informatique en proposant les services nécessaires au traitement des incidents et en aidant leurs parties prenantes à restaurer les systèmes qui en ont fait l'objet (*Guide de création d'un CSIRT pas à pas* disponible à l'adresse suivante: www.enisa.europa.eu/act/cert). Les CSIRT sont aussi parfois appelés *Computer Emergency Response Teams* ou *Computer Emergency Readiness Teams* (CERT), les CSIRT et les CERT réalisant la même fonction. Dans ce rapport, le terme "ordinateur" utilisé dans un CSIRT désigne à la fois, par exemple, les routeurs, les serveurs, les dispositifs mobiles IP et les applications associées.

[10] Aux fins du présent Rapport, un CSIRT national sera désigné par le sigle "CIRT".

formateurs. Ces forums servent à mieux faire connaître les problèmes, donnent lieu à des présentations d'experts et permettent aux pays de partager leurs idées, leurs expériences et leurs perspectives. La participation et/ou l'adhésion à des organisations régionales ou internationales qui partagent les mêmes buts peuvent également concourir à cet effort. Tel est l'un des objectifs du projet de la Résolution 45.

2. La participation aux programmes et activités disponibles d'organisations multilatérales qui visent à améliorer et à renforcer la cybersécurité au niveau mondial est une autre façon d'encourager la collaboration internationale. Autres exemples d'organisations multilatérales: L'Union internationale des télécommunications (grande orientation C5 du Plan d'action du SMSI), l'Organisation de coopération et de développement économiques (OCDE), l'Organisation des Etats américains (OEA), l'Organisation de coopération économique Asie-Pacifique (APEC), etc. De plus, il existe d'autres conférences où les gouvernements peuvent échanger des informations sur les questions de cybersécurité comme la *Meridian Conference*.

3. En outre, la participation aux activités du secteur privé, comme le Anti-Phishing Working Group et d'autres efforts déployés au niveau international, devraient être pris en considération.

I.B.7 Elaborer un processus intégré de gestion des risques pour identifier les mesures de protection à adopter en matière de cybersécurité et les classer par ordre de priorité.

1. Ce n'est qu'en comprenant les risques que les pouvoirs publics ainsi que les propriétaires et les opérateurs d'infrastructures (y compris les constructeurs qui les soutiennent) peuvent amorcer une collaboration pouvoirs publics/privés en vue d'identifier les fonctions et éléments décisifs à protéger et d'en établir l'ordre de priorité. Une fois identifiées, les fonctions de l'infrastructure essentielle de l'information peuvent être hiérarchisées ou classées selon leur importance et leur contexte. Il convient de rappeler que la notion de caractère "essentiel" dépend de la situation et que ce qui peut s'avérer essentiel dans un cas peut ne pas l'être dans un autre. A mesure que les pays recensent et classent les fonctions essentielles par ordre de priorité, ils doivent se souvenir que la notion précitée évoluera selon les technologies, les infrastructures et l'évolution.

2. Assurer la protection de la CII et du cyberespace est une tâche très ardue. La protection de la CII et du cyberespace ainsi que des fonctions essentielles qui les composent suppose l'application ininterrompue d'une série de pratiques de gestion des risques (c'est-à-dire, évaluation des menaces, des vulnérabilités et des conséquences, identification des mesures de contrôle et d'intervention, mise en œuvre des mesures de contrôle et évaluation de l'efficacité) qui permettent aux opérateurs de gérer les risques et d'assurer leur adaptabilité dans l'exécution de leurs tâches essentielles. A titre individuel, les fournisseurs d'infrastructures de l'information disposent en général de méthodologies et de pratiques perfectionnées de gestion des risques en raison du caractère instantané des services qu'ils fournissent. Toutefois, l'interconnectivité, l'interdépendance et la complexité technique de cette infrastructure limitent la possibilité d'évaluer aisément le risque global ou la propension au risque. De ce fait, il y a avantage à tirer parti de la coopération entre le secteur public et le secteur privé pour évaluer les dépendances mutuelles et les risques liés à l'infrastructure (catastrophe naturelle, défaillance technologique, attaque terroriste, etc.).

I.B.8 Evaluer et réévaluer périodiquement l'état de la cybersécurité et développer des priorités de programme.

1. La stratégie nationale en matière de cybersécurité devrait comprendre une étude nationale d'évaluation, qui pourrait être utilisée pour l'auto-évaluation des progrès réalisés, dans le cadre de l'effort de formation ou encore de l'effort d'évaluation considéré. En utilisant un outil d'auto-évaluation commun, les pays peuvent identifier les avantages et les lacunes potentiels de leur cadre national et élaborer un processus qui permet de les mettre en adéquation avec les objectifs souhaités (un outil d'auto-évaluation, le kit pratique de l'UIT pour l'autoévaluation relative à la cybersécurité/CIIP au niveau national, a été élaboré par le BDT pour accompagner le présent document sur les bonnes pratiques).

I.B.9 Identifier les besoins de formation et la façon d'y pourvoir.

1. En comparant les bonnes pratiques recommandées dans le présent rapport et ses pratiques actuelles dans le domaine de la cybersécurité (c'est-à-dire en menant une analyse d'écart), un pays peut constater que certains aspects de son programme de cybersécurité doivent être améliorés. La solution peut être technique (de nouveaux matériels ou logiciels, par exemple), juridique (préparer de nouvelles lois ou réglementations pour faire face à des comportements inadéquats sur le net, par exemple) ou organisationnelle. Il y a aussi des chances pour qu'une analyse d'écart montre où il est nécessaire de renforcer les capacités humaines (formation).

PARTIE II

Etablir une collaboration au niveau national entre les pouvoirs publics et le secteur privé

La protection des infrastructures essentielles de l'information et du cyberespace est une responsabilité partagée qui peut s'avérer optimale si elle s'appuie sur une collaboration entre les pouvoirs publics à tous les niveaux et le secteur privé, qui possède et exploite une grande partie de l'infrastructure. Les gouvernements possèdent évidemment le dernier mot sur les décisions nationales qui ont été prises. Il est important de reconnaître que si les systèmes de sécurité de l'information du monde entier forment désormais, pour l'essentiel, un ensemble interopérationnel et interconnecté, la structure de ce réseau peut varier énormément d'un pays à l'autre. Par conséquent, un système de sécurité efficace et durable pourra être amélioré grâce à une collaboration entre les propriétaires et les opérateurs de ces systèmes.

L'intérêt que les pouvoirs publics et le secteur privé ont d'assurer la résilience de l'infrastructure ne se dément pas. Par conséquent, la collaboration entre les pouvoirs publics et le secteur privé est indispensable pour renforcer la cybersécurité car aucune entité à elle seule ne peut protéger la totalité de l'infrastructure. Une grande partie de l'infrastructure électronique étant, dans nombre de pays, la propriété du secteur privé et/ou exploitée par lui, il est recommandé que les pouvoirs publics et le secteur privé travaillent ensemble d'une manière significative en fonction du rôle qui leur est dévolu. Pour que cette collaboration soit réussie, trois éléments sont importants: 1) une proposition de valeur; 2) des rôles et des responsabilités clairement définies; et 3) la confiance.

Proposition de valeur

Le partenariat sera couronné de succès si les avantages mutuels sont clairement spécifiés aux partenaires que sont les pouvoirs publics et le secteur privé. Il est avantageux pour les pouvoirs publics que les fournisseurs et les opérateurs de l'infrastructure mettent à disposition des moyens qui sortent en général des compétences fondamentales des pouvoirs publics, à savoir:

- Propriété et gestion de la plupart des infrastructures essentielles dans de nombreux secteurs, dans beaucoup de pays.
- Connaissance des ressources, réseaux, systèmes, installations, fonctions et autres moyens.
- Compétences et expérience pour réagir aux incidents informatiques.
- Aptitude à innover et à proposer des produits, des services et des technologies pour répondre rapidement aux besoins.
- Conception, déploiement, exploitation, gestion et maintenance du réseau Internet mondial.

Lorsqu'on évalue la proposition de valeur pour le secteur privé, il est manifestement avantageux de travailler avec les pouvoirs publics pour renforcer la CIIP et la cybersécurité. En effet, les pouvoirs publics peuvent valoriser à plus d'un titre cette collaboration, notamment:

- en fournissant, en temps utile, aux propriétaires et aux opérateurs un ensemble d'informations analytiques, précises et utiles sur les menaces qui pèsent sur l'infrastructure essentielle;
- en invitant le secteur privé, dès le début, à élaborer des initiatives et des politiques en matière de TIC;
- en exposant aux dirigeants des entreprises, dans le cadre de tribunes publiques et par des communications directes, les avantages, tant pour l'entreprise qu'au niveau de la sécurité nationale, qu'il y a d'investir dans des mesures de sécurité qui dépassent les stratégies propres à telle ou telle entreprise;

- en créant un environnement qui encourage et incite les entreprises à adopter, sur une base volontaire, des pratiques saines de sécurité qui sont largement reconnues et, le cas échéant, à actualiser et améliorer leurs activités et pratiques en matière de sécurité pour dépasser les intérêts centrés sur ces entreprises;
- en œuvrant avec le secteur privé pour définir des activités fondamentales et les hiérarchiser et permettre leur protection et/ou rétablissement;
- en fournissant un appui pour les recherches nécessaires en vue de renforcer les efforts futurs en matière de protection des CI;
- en définissant les ressources à engager dans les études d'interdépendance intersectorielle, par des exercices, des colloques, des stages et une modélisation informatique afin d'aboutir à des décisions éclairées pour une planification suivie des entreprises;
- en permettant l'échange d'informations d'actualité ainsi que la mise en place de mesures de rétablissement des installations et services d'infrastructure prioritaires lors d'un incident.

Rôles et responsabilités

L'administration et le secteur privé peuvent, ensemble, se mettre d'accord sur les rôles et les responsabilités qu'elles doivent déployer en ce qui concerne la cybersécurité. L'administration peut assurer la coordination et la conduite des actions de protection. La pérennité de l'administration, par exemple, oblige à garantir la sécurité et la disponibilité des infrastructures électroniques et physiques pour appuyer ses missions et services essentiels. De plus, l'administration peut jouer un rôle de coordinateur déterminant lors d'une catastrophe, ou peut apporter son appui lorsque le secteur privé ne dispose pas des ressources suffisantes pour intervenir en cas d'incident. L'administration peut promouvoir et encourager des mesures prises sur une base volontaire par le secteur privé pour améliorer la sécurité, y compris en instaurant les politiques et les protocoles nécessaires au partage en temps voulu d'informations analytiques et utiles concernant les menaces, et en incitant le secteur privé à améliorer la sécurité au delà des intérêts des entreprises. Enfin, le gouvernement peut parrainer et financer des études et la recherche-développement afin d'améliorer les processus et outils de sécurité.

Confiance

La confiance est un élément fondamental d'une collaboration réussie entre les pouvoirs publics et le secteur privé. Elle est nécessaire à la création, au développement et à l'entretien de relations de partage entre les pouvoirs publics et le secteur privé. Une collaboration et des échanges d'informations solides entre le secteur privé et l'administration augmentent la sensibilisation situationnelle, facilitent la coopération sur des questions stratégiques, permettent de gérer le risque électronique et de soutenir les activités de réponse et de retour à la normale. Grâce à des partages et à des analyses d'informations améliorés, les secteurs public et privé seront mieux équipés pour identifier les menaces et les vulnérabilités ainsi que pour échanger des tactiques et des ressources correctives et préventives.

On trouvera ci après la liste des objectifs généraux que les gouvernements devraient prendre en considération lorsqu'ils collaborent avec le secteur privé.

II.A Aperçu des objectifs de cette partie

II.A.1 Instaurer des relations de collaboration entre les pouvoirs publics et le secteur privé pour gérer efficacement le risque électronique et protéger le cyberespace.

II.A.2 Offrir un mécanisme permettant la mise en place de toute une série de propositions, actions et connaissances afin de dégager un consensus et d'aller de l'avant en vue d'améliorer la sécurité au niveau national.

II.B Mesures spécifiques pour atteindre ces objectifs

II.B.1 Intégrer les vues du secteur privé dans les premières étapes du développement et de la mise en œuvre de la politique de sécurité et des mesures associées.

1. Dans de nombreux pays, les infrastructures les plus essentielles, ainsi que les éléments électroniques sur lesquels elles reposent, sont la propriété du secteur privé, qui les met aussi en œuvre. Les technologies qui créent et prennent en charge le cyberespace évoluent rapidement grâce aux innovations du secteur privé. Par conséquent, les pouvoirs publics à eux seuls ne peuvent pas sécuriser suffisamment le cyberespace. La sensibilisation aux perspectives du secteur privé et la participation des principaux propriétaires et opérateurs de l'infrastructure essentielle sont extrêmement précieuses pour les actions menées par l'administration en vue de développer et de mettre en œuvre une politique de cybersécurité ainsi que des cadres pour la gestion des risques. Les pouvoirs publics peuvent être informés par le secteur privé en participant à des groupes de travail pouvoirs publics/secteur privé, en sollicitant les commentaires du secteur privé sur le développement d'une politique et d'une stratégie de cybersécurité et en coordonnant les actions avec les organisations du secteur privé au travers de mécanismes de partage d'informations. Le gouvernement devrait s'assurer que le secteur privé est impliqué aussi en amont que possible dans le développement, la mise en œuvre et la continuité des initiatives et des politiques.

2. Les pouvoirs publics et le secteur privé devraient adopter conjointement une méthode de gestion des risques pour permettre à l'administration et au secteur privé d'identifier l'infrastructure électronique, d'analyser les menaces, d'évaluer les vulnérabilités et les conséquences, et enfin, d'identifier les mesures d'intervention.

3. Les pouvoirs publics et le secteur privé devraient déployer ensemble des activités de recherche développement (R&D) pour gérer les risques électroniques. Faire mieux connaître les priorités et les initiatives de R&D adoptées par le secteur privé et l'administration peut permettre de garantir que les ressources sont attribuées et utilisées efficacement, que les initiatives de R&D sont élaborées en temps opportun et, finalement, que les produits et services seront disponibles à temps pour améliorer la cybersécurité nationale.

II.B.2 Encourager la constitution de groupes du secteur privé provenant de divers secteurs des infrastructures essentielles, pour appréhender les intérêts communs dans le domaine de la sécurité, en collaboration avec les pouvoirs publics.

1. La création de ces groupes, comme des associations professionnelles, dans divers secteurs des infrastructures essentielles, peut aider à faire face aux besoins communs de cybersécurité. Ces groupes peuvent se concentrer sur des questions stratégiques et/ou opérationnelles ainsi que sur la gestion des problèmes de sécurité relatifs au secteur privé dans son ensemble. Ces questions peuvent inclure la gestion des risques, la sensibilisation, le développement et la mise en œuvre d'une politique ainsi qu'une multitude d'autres sujets. Ces groupes du secteur privé fournissent un processus institutionnalisé d'engagement auprès de l'administration et peuvent servir de forum pour les concertations délicates sur les questions de cybersécurité.

2. Dans certains pays, des groupes ont été créés par plusieurs secteurs des infrastructures essentielles afin d'amener des représentants sectoriels à partager des informations sur les menaces, les vulnérabilités et les impacts concernant la sécurité. Souvent, ces groupes ont également fourni des alertes en temps réel et des mises en garde à leurs membres afin de faciliter les efforts pour atténuer des incidents réels impactant les infrastructures essentielles, y répondre et revenir à la normale.

3. Ces groupes devraient envisager d'adopter des pratiques permettant d'instaurer une collaboration et un échange d'informations entre les membres (c'est-à-dire, pouvoirs publics et secteur privé) dans un forum "de confiance ". Certaines de ces pratiques peuvent comprendre notamment les suivantes: assurer l'anonymat des membres, l'accès à des informations intersectorielles et de l'administration, l'accès à des menaces sensibles, à des vulnérabilités et à des produits analytiques, et enfin, fournir des connaissances spécialisées sur la coordination des interventions d'urgence, les pratiques de fonctionnement et exercices. Tout en tenant compte de ces pratiques pour permettre la collaboration, il est important d'inclure des moyens de protéger les informations propres aux entreprises ou sensibles pour elles.

II.B.3 Réunir des groupes sectoriels et l'administration dans des forums "de confiance" afin d'examiner les problèmes communs de cybersécurité.

1. Plusieurs conditions sont nécessaires pour créer la confiance et favoriser le succès de la collaboration entre l'administration et le secteur privé. Il est recommandé d'avoir un accord écrit qui oriente la collaboration et les échanges entre l'administration et le secteur privé. Les parties prenantes ont besoin d'une vision et d'un but partagés. Le leadership fort d'une personne physique ou d'une organisation permet de fixer des priorités, de répartir les ressources et de prendre les engagements nécessaires au soutien de la collaboration pouvoirs publics/secteur privé. Un règlement est également nécessaire pour orienter le comportement des personnes physiques et des organisations dans la relation de collaboration.

2. Les parties prenantes doivent voir des résultats concrets et mesurables. Il est déterminant pour le développement et la poursuite de la collaboration pouvoirs publics/secteur privé d'indiquer les avantages de la collaboration et d'en formuler clairement l'utilité pour les personnes physiques et les organisations.

II.B.4 Encourager la coopération entre des groupes de secteurs d'activité interdépendants.

1. Des incidents impliquant une catégorie d'infrastructure peuvent avoir des effets en cascade et aboutir à des incidents dans d'autres catégories d'infrastructure. Les coupures de courant, par exemple, peuvent interrompre les services du téléphone et de l'Internet. De plus, bien que l'on puisse prévoir des cas d'urgence dans son propre secteur, il faut aussi tenir compte de l'impact que les incidents peuvent avoir sur d'autres secteurs. Partager des informations entre les infrastructures peut contribuer aux efforts qui visent à répondre aux incidents touchant de multiples secteurs et qui sont significatifs à l'échelle nationale.

II.B.5 Etablir des arrangements coopératifs entre l'administration et le secteur privé pour la gestion des incidents.

1. Une identification rapide, un échange d'informations et des mesures correctives peuvent souvent réduire le dommage causé par des incidents électroniques. Une collaboration pouvoirs publics/secteur privé est nécessaire sur le plan national pour mener des études, émettre des alertes et coordonner les actions de réponse.

2. Les pouvoirs publics et l'industrie devraient collaborer au développement d'un cadre de coordination à des fins stratégique, opérationnelle et de sensibilisation pour améliorer la gestion des incidents. Ce cadre devrait s'articuler sur un concept formel de partage des informations qui englobe les responsables des questions de politique et de l'échange d'informations à caractère opérationnel. Il devrait aussi englober des politiques et des procédures permettant de signaler les incidents, de protéger et de diffuser des informations sensibles, propres aux pouvoirs publics et au secteur privé, ainsi que des mécanismes de communication et de diffusion de l'information. Les informations détenues par le secteur privé contiennent souvent des données propres aux sociétés qui, si elles étaient divulguées au public, pourraient aboutir à la perte d'une part de marché, à de la contre-publicité ou avoir d'autres conséquences négatives. De la même façon, les informations détenues par les pouvoirs publics peuvent être confidentielles ou sensibles et à ne pas divulguer au public. Il conviendrait de mettre en place une politique et des mesures techniques pour protéger les informations, tout en tenant compte du droit du public à disposer d'informations. Les gouvernements peuvent continuer à développer la confiance en renforçant les politiques de partage de l'information et les relations pouvoirs publics/secteur privé par une évaluation continue des politiques. Des exercices électroniques permettent aussi de tester les communications entre les pouvoirs publics et le secteur privé, la coordination concernant les interventions en cas de cyberincidents et les efforts de rétablissement par la mise en œuvre de mécanismes en période de crise réelle.

PARTIE III

Prévenir la cybercriminalité

On peut améliorer sensiblement la cybersécurité, notamment en élaborant et en modernisant le droit pénal ainsi que les procédures et la politique pénale pour prévenir, empêcher la cybercriminalité mais aussi réagir face à cette menace et engager des poursuites en la matière.

III.A Aperçu de l'objectif de cette partie

III.A.1 Promulguer et mettre en vigueur une série de lois relatives à la cybersécurité et à la cybercriminalité.

Chaque pays a besoin d'une législation qui traite de la cybercriminalité en soi, de procédures d'investigation électronique et d'assistance aux autres pays. Cette législation peut être située ou non en un seul endroit dans les codes d'un pays. Par souci de simplicité, le présent document présume que chaque pays aura une loi principale sur la cybercriminalité, plus une série de textes juridiques connexes sur la procédure et l'assistance mutuelle. Bien évidemment, les pays utiliseront la structure qui, à leur avis, répond le mieux à leurs spécificités.

III.B Mesures spécifiques pour atteindre cet objectif

III.B.1 Evaluer l'adéquation des instances judiciaires actuelles. Il conviendrait qu'un pays examine son code pénal, y compris les procédures pertinentes, afin de déterminer s'il convient pour résoudre les problèmes actuels (et futurs). Mesures suggérées:

1. Elaborer, le cas échéant, la législation pertinente nécessaire, en tenant compte en particulier des initiatives prises au niveau régional. Cette loi devrait notamment traiter des dommages causés aux données informatiques ou de leur destruction; des procédures à adopter pour lancer des recherches, y compris la possibilité de retracer l'origine des messages de courriers électroniques, etc., et notamment la question d'une éventuelle coopération internationale (par exemple, pour fournir des preuves, etc.).
2. Un pays devrait examiner si ses lois reposent sur des attentes technologiques dépassées. Par exemple, une loi peut débattre du traçage des seules transmissions vocales. Elle pourrait devoir être modifiée pour s'étendre aussi aux transmissions de données.
3. La législation d'un pays sur la cybercriminalité devrait être évaluée par toutes les autorités gouvernementales et organes législatifs pertinents qui pourraient y trouver un intérêt, même s'ils ne sont pas concernés par la justice pénale, afin qu'aucune idée utile ne soit omise. Un responsable du secteur des technologies de l'information pourrait remarquer, par exemple, que la législation sur la cybercriminalité ne s'étend pas à une nouvelle technologie dont l'utilisation est croissante mais qui n'est pas encore bien connue des rédacteurs juridiques du pays considéré.
4. En outre, il est recommandé que la législation nationale existante sur la criminalité fasse de la même façon l'objet d'une évaluation de la part de certains ou de l'ensemble des acteurs suivants: le secteur privé local, une filiale locale du secteur privé international, des organisations non gouvernementales locales, des universitaires et des experts reconnus ou des groupes de citoyens.
5. Un pays peut rechercher auprès d'autres pays un conseil sur ces questions.

III.B.2 Rédiger et adopter des textes de droit matériel, procédural et d'assistance mutuelle et des politiques visant à traiter la cybercriminalité.

1. Recommander que les pays participent activement à l'élaboration, le cas échéant, de la législation nécessaire, en tenant compte en particulier des initiatives régionales dont la Convention du Conseil de l'Europe sur la cybercriminalité, mais pas uniquement. Recommander que les pays collaborent aux niveaux régional et international afin de lutter contre la cybercriminalité et de renforcer la

cybersécurité et élaborent des mécanismes propres à renforcer la coopération en matière de cybersécurité, y compris lutter contre le spam, les maliciels, les botnets, etc.

2. Le projet de loi d'un pays sur la cybercriminalité devrait être évalué par l'ensemble des autorités gouvernementales et des organes législatifs. Un tel projet devrait également être rendu public afin de recueillir des observations qui permettront de traiter des technologies, infractions ou autres questions éventuelles dont il n'a pas été tenu compte à l'origine.

3. Toute législation sur la cybercriminalité devrait traiter non seulement les cyberdélits classiques, comme les délits informatiques et les intrusions dans les systèmes informatiques, mais également protéger les éléments de preuve électroniques sur réseaux relatifs à d'autres délits.

4. Les lois sur la protection des données conçues pour la vie civile et pour la vie des affaires ne devraient pas être étendues ou interprétées dans le but de gêner indûment le flux des preuves criminelles entre les pays.

5. Les pays qui décident d'employer des consultants pour rédiger le projet devraient étudier leurs qualifications et superviser leur travail tout au long du processus. Les personnes qui n'ont pas été formées spécialement selon la législation d'un pays risquent de ne pas bien intégrer toutes les dispositions nécessaires, particulièrement en ce qui concerne les articles sur la procédure et l'assistance juridique mutuelle. De plus, il y a peu de chances pour que les personnes qui n'ont pas d'expérience en matière de poursuites tiennent dûment compte des détails pratiques de la démonstration d'une preuve. Certains consultants sont qualifiés pour aider à la rédaction de projets de loi sur le commerce électronique mais pas pour ceux qui concernent le droit pénal.

6. D'autres pays pourraient être consultés afin de recueillir des suggestions au-delà de ce qui est inclus dans la Convention. Les pays peuvent, par exemple, demander aux fournisseurs de services Internet de conserver pendant un certain temps, 6 mois le plus souvent, certaines des données qui transitent dans leurs systèmes ou bien ils peuvent exiger que les incidents informatiques d'une certaine importance soient signalés aux autorités gouvernementales, ou encore ils peuvent exiger une identification des personnes utilisant les services d'un cybercafé.

7. S'il en a le temps, un pays pourrait demander l'avis d'autres pays et d'organisations multilatérales sur son projet de loi sur la cybercriminalité (ou sur les projets d'amendement). Ces commentaires peuvent être obtenus de façon privée et, comme indiqué ci-dessus, il est utile d'obtenir les points de vue de plusieurs pays fondés sur leur expérience.

8. Un pays devrait également chercher à obtenir le plus tôt possible (en fonction des procédures nationales) les commentaires des entités concernées ayant un intérêt reconnu en la matière: le secteur privé local, une filiale locale du secteur privé international, des organisations non gouvernementales locales, des universitaires, des citoyens indépendants intéressés, etc.

III.B.3 Instaurer ou identifier des unités nationales spécialisées en cybercriminalité.

1. Il est important que chaque pays, indépendamment de son niveau de développement, dispose au moins d'une capacité d'enquête de base dans le domaine de la cybercriminalité. Par exemple, l'utilisation de téléphones mobiles a explosé même dans les pays en développement, sachant que ces téléphones peuvent servir à commettre des fraudes, transférer de l'argent, conspirer, transmettre des virus à des réseaux électroniques, déclencher des explosifs, etc.

2. Chaque pays devrait sélectionner ou former un ou plusieurs services de police qui auront compétence pour enquêter en matière de cybercriminalité nationale. Parfois, le choix sera évident. Parfois, des forces de police concurrentes lutteront pour être sélectionnées et les autorités supérieures auront à prendre une décision difficile. Même s'il semble que le pays n'a actuellement personne de compétent, il y a en général toujours un fonctionnaire de police quelque part qui s'intéresse à l'électronique et qui désire approfondir ses connaissances et progresser dans ce domaine.

3. Les unités d'enquête spécialisées en cybercriminalité, même si elles ne comprennent qu'un nombre limité d'enquêteurs, ont besoin d'un appui. Elles ont besoin de matériels relativement récents, de connexions au réseau raisonnablement fiables et de formation continue. Cet appui peut provenir du

gouvernement du pays, d'organisations internationales ou d'autres pays, et de donations du secteur privé.

4. Si possible, il est souhaitable que les unités disposent au moins des moyens essentiels de police scientifique appliquée à l'informatique et, partant, d'outils logiciels et d'une formation complémentaire. (Si l'on considère que des moyens de police scientifique ne peuvent pas être mis en place, les pays devraient accepter d'avance que des preuves capitales, même dans des affaires cruciales, puissent être perdues.) Dans certaines circonstances, une assistance en police scientifique sur des affaires particulières pourrait être obtenue d'autres pays. En outre, une formation aux techniques de police scientifique peut être obtenue de la part d'autres pays et d'organisations pertinentes. Par exemple, le Computer Emergency Response Team Coordination Center de l'Université Carnegie-Mellon aux Etats-Unis (www.cert.org) offre des formations aux techniques de police scientifique gratuites ou à des prix très modérés, en ligne ou sur CD-ROM.

5. Lorsqu'une unité de cybercriminalité est constituée, elle devrait faire connaître son existence et ses capacités aux autres services de police et aux procureurs du pays. Il est inutile de disposer d'une unité de cybercriminalité dans la capitale si une force de police régionale enquêtant sur un crime horrible impliquant des preuves électroniques ne sait pas qu'il existe une unité de cybercriminalité capable de rechercher l'ordinateur de la cible ou d'offrir d'autres ressources. Malheureusement, il est très courant, partout dans le monde, que les pouvoirs de police d'un pays ignorent que le pays dispose d'une unité de cybercriminalité.

6. Les unités de cybercriminalité existantes ou à venir devraient encourager au maximum les contacts avec des partenaires internationaux. Au début, on peut obtenir des avis sur la création de l'unité auprès d'autres pays et d'organisations policières internationales. Par la suite, des formations diverses et même du matériel et des logiciels seront disponibles auprès d'autres pays, d'organisations policières internationales, d'organisations multilatérales pertinentes et du secteur privé. Ces contacts seront précieux également pour une autre raison: dans un monde qui va de plus en plus fonctionner en réseau, il est fondamental de pouvoir demander de l'aide à des pouvoirs de police étrangers.

7. Les unités de cybercriminalité devraient également prendre contact avec tout secteur pertinent et intéressé dans leurs pays, par exemple les organisations non gouvernementales nationales, les CSIRT, les entités du secteur privé et le monde universitaire, pour veiller à ce que ces différents organismes connaissent l'existence et les capacités desdites unités, puissent collaborer avec elles et comprendre comment rendre compte des éventuelles infractions commises.

III.B.4 Développer des relations coopératives avec d'autres composantes de l'infrastructure de cybersécurité nationale et avec le secteur privé.

1. Les relations coopératives entre autorités gouvernementales, autres composantes de l'infrastructure de cybersécurité nationale et secteur privé sont importantes pour plusieurs raisons:

   a) échanger des informations entre ces groupes (pour être au courant, par exemple, qu'une nouvelle loi est envisagée ou qu'une nouvelle technologie est en cours de développement);

   b) échanger des opinions (par exemple: "Si nous élaborons une nouvelle loi de ce genre, y verriez-vous des problèmes de respect de la vie privée?" ou "Pouvez vous modifier cette technologie afin que l'on puisse pister des courriels si des raisons de sécurité publique légitimes sont invoquées?");

   c) échanger des formations, même si, la plupart du temps, elles seront offertes par le secteur privé à l'administration publique;

   d) échanger des alertes concernant des menaces ou des vulnérabilités;

   e) agir de façon que des gens de divers secteurs apprendront à se connaître suffisamment pour se faire confiance dans des situations d'urgence.

2. Une ou plusieurs personnes peuvent réaliser une première démarche intéressante à l'occasion de ces prises de contact en établissant un répertoire des personnes et organisations ayant telle ou telle compétence de l'Internet dans tous les secteurs du pays. Les coordonnées de ces personnes peuvent être indiquées dans le répertoire afin qu'elles puissent être contactées. Il est probablement préférable

que ce répertoire reste informel afin d'éviter les débats sur la question de savoir qui figure dans le répertoire et qui n'y figure pas.

3. Dans chaque pays, il est probable que de nombreux secteurs pertinents ont une vision utile de la cybersécurité – les législateurs, les ministères, les organisations non gouvernementales, les CSIRT, le monde universitaire, le secteur privé et les particuliers. Certains d'entre eux peuvent avoir une dimension entièrement nationale alors que d'autres peuvent être affiliés à des entités étrangères plus grandes.

III.B.5 Développer une compréhension des questions de cybercriminalité auprès des procureurs, des juges et des législateurs.

1. Pour chercher à résoudre correctement les questions de cybercriminalité, il est important que les procureurs et les juges possèdent des connaissances dans certains domaines, tels que l'informatique, les logiciels et les réseaux et soient informés de l'importance croissante des preuves électroniques. De même, les législateurs devraient avoir des connaissances de ces sujets et savoir si les lois de leur pays permettent de traiter de la cybercriminalité. La formation est une solution à ce problème.

2. Si une formation technique élémentaire est nécessaire, elle peut être dispensée par divers organismes, selon les ressources du pays:

   a) n'importe quel service intérieur ou ministère ayant une compétence technique, tel qu'un service de police ou un ministère des technologies de l'information;

   b) des gouvernements étrangers;

   c) des organisations multinationales pertinentes;

   d) le secteur privé local;

   e) le secteur privé international, particulièrement (mais pas exclusivement) s'il a des activités locales;

   f) des organismes universitaires pertinents;

   g) les centres nationaux ou étrangers d'alerte et de réaction aux attaques informatiques; et

   h) les organisations non gouvernementales nationales et étrangères pertinentes.

3. Il peut aussi être utile de former les décideurs de niveau supérieur, les fonctionnaires, etc., aux menaces qui existent envers les réseaux électroniques (comment le système bancaire national pourrait être attaqué, par exemple) et aux menaces posées par les réseaux électroniques (utilisation de l'Internet pour localiser des enfants vulnérables afin de faire du trafic sexuel, par exemple). La formation à ces aspects des réseaux électroniques devrait être disponible auprès des sources ci-dessus.

4. Des formations peuvent être demandées pour les procureurs et les juges au sujet des poursuites dans le domaine de la cybercriminalité ou autre sorte de criminalité impliquant des preuves électroniques, ou de l'utilisation de la preuve électronique, ou des méthodes pour obtenir une coopération internationale. Des formations de ce genre peuvent être obtenues auprès:

   a) de tout service ou ministère national disposant de la compétence adéquate, comme un parquet ou un ministère de la justice;

   b) des gouvernements étrangers;

   c) des organisations multinationales pertinentes;

   d) des organismes universitaires pertinents;

   e) des organisations non gouvernementales nationales et étrangères pertinentes; et

   f) des particuliers pertinents.

5. Un pays peut désirer recevoir une formation à la rédaction des projets de loi. Celle-ci peut être obtenue auprès des groupes énumérés ci-dessus. Le secteur privé local et le secteur privé international, particulièrement (mais pas exclusivement) s'il a des activités locales, peuvent être des sources de compétences. Cependant, il y a plus de chances que les entités du secteur privé puissent

fournir une aide dans le domaine du droit commercial que dans ceux de la cybercriminalité, de la procédure pénale et de la législation sur l'entraide juridique internationale.

6. Pour tous ces types de formation, les sources peuvent offrir d'assurer elles-mêmes la formation dans le pays demandeur où elles peuvent offrir des modules de formation (électroniques ou imprimés) dont les instructeurs de ce pays pourront se servir en dispensant eux-mêmes la formation. Dans certains cas, comme pour la formation CERTCC décrite au § III.B.3.4, une telle formation peut être dispensée gratuitement ou à moindres frais.

7. Dans certains pays, la clé de la sensibilisation nationale aux problèmes de cybercriminalité a été le soutien de hauts fonctionnaires, ou parfois même d'un seul haut fonctionnaire, disposant d'un pouvoir important, en particulier ceux qui contrôlent les budgets. Si un ministre a la réputation d'être très intéressé par la cybersécurité, son ministère – et peut-être le reste du gouvernement – peuvent apporter un meilleur soutien aux employés qui essaient de réaliser quelque chose dans le domaine.

III.B.6 Participer au réseau 24/7 des points de contact de la cybercriminalité.

1. En 1997, le Subgroup on High-Tech Crime du groupe des huit pays industrialisés (G8) a mis sur pied le réseau 24/7 des points de contact de la cybercriminalité sur la demande des ministères de la Justice et de l'Intérieur du G8 pour améliorer l'entraide internationale dans les enquêtes urgentes impliquant des preuves électroniques. Beaucoup d'enquêteurs de la cybercriminalité étaient d'avis qu'il était trop difficile d'apprendre où obtenir une entraide rapide de la part d'autres pays. De plus, bon nombre d'enquêteurs estimaient que des traités d'entraide vieux de dizaines d'années n'étaient d'aucune utilité dans des affaires qui évoluent rapidement impliquant, par exemple, des intrusions informatiques en pleine nuit dans les systèmes financiers d'un pays. Ce réseau a grandi jusqu'à inclure près de 50 pays début 2008. Le réseau est ouvert à tout pays qui a la capacité nécessaire d'assistance décrite ci dessous.

2. Pour adhérer au réseau, les pays doivent offrir un point de contact accessible 24 heures sur 24, 7 jours sur 7, d'où son nom informel, "le réseau 24/7". Le point de contact peut être une personne joignable directement ou via un service. Elle doit posséder des connaissances de différents ordres: 1) technologique, afin que les demandes puissent être transmises sans nécessiter de longues explications techniques; 2) juridique: son propre droit national; et enfin, 3) savoir ce que la législation nationale lui permet de faire pour aider d'autres pays. Si le point de contact n'a pas ces trois sortes de savoir, il doit être capable de contacter immédiatement (pas simplement le jour ouvrable suivant), si nécessaire, la personne compétente de son administration habilitée à lui venir en aide.

3. Les communications doivent aller, du moins au début, du point de contact 24/7 du pays A vers le point de contact 24/7 du pays B afin de garantir cohérence et sécurité. Cela signifie que les points de contact ne devraient pas faire part de leurs informations de contact à d'autres services dans leurs propres pays. Plus exactement, les points de contact devraient assurer leur premier contact international au nom d'un service demandeur (une force de police provinciale, par exemple) de leur pays. Après l'établissement d'une coopération initiale entre deux pays, un point de contact peut, si cela lui est demandé, se retirer de l'enquête et laisser l'organisme de police provinciale pertinent du pays A communiquer directement avec le pays B.

4. En adhérant au réseau, les pays ne garantissent pas qu'ils s'entraideront toujours, ni que le réseau de contacts remplacera l'entraide normale entre pays. Plus précisément, ledit réseau garantit seulement qu'un pays demandeur bénéficiera immédiatement d'une attention intelligente et compétente, même en pleine nuit. Après un début d'entraide, les pays peuvent (ou non) demander que des canaux d'entraide moins rapides soient utilisés.

5. Une disponibilité 24 heures sur 24 ne veut pas dire qu'un service est doté jour et nuit de stations de travail et de cyberenquêteurs qui attendent pour répondre à des appels téléphoniques ou à des courriels. La plupart des pays ne disposent pas d'un tel service. Plus couramment, un fonctionnaire de police (ou peut-être plusieurs exerçant en rotation) d'un pays sera joignable par téléphone – dormant peut-être avec un téléphone portable près de lui.

6. Pour adhérer, les pays doivent contacter le président du High-Tech Crime Subgroup du G8 (l'adhésion n'est pas limitée aux membres du G8; de fait, près de 50 pays en font déjà partie). Un formulaire simple et court doit être rempli[11]. Le processus n'exige pas d'accords internationaux formels tels que des mémorandums d'accord ou des traités. De temps à autre, le réseau 24/7 propose des conférences de formation et de prise de contact destinées aux points de contact. Les déplacements pour ces conférences sont subventionnés selon les besoins.

7. Il appartient à l'unité qui adhère au réseau de faire savoir aux autres services de police intéressés ou aux unités de cybercriminalité de son pays qu'elle existe et qu'elle est prête à aider à prendre des contacts hors du pays.

---

[11] Le formulaire doit être envoyé par fax au numéro +1 202-514-6113, adressé à "Coordinator, 24/7 Network, Computer Crime and Intellectual Property Section, US Dept. of Justice, Washington, D.C., U.S.A." Il peut également être envoyé par courrier électronique à l'adresse richard.green@usdoj.gov

PARTIE IV

Créer au niveau national des structures de gestion des incidents: surveillance, alerte, intervention et retour à la normale

Il est important pour l'administration de créer ou d'identifier une organisation nationale qui serve de point de convergence pour la sécurisation du cyberespace et la protection de l'infrastructure essentielle de l'information, dont la mission comprend des activités de surveillance, d'alerte, d'intervention et de retour à la normale et vise aussi à encourager la collaboration entre les entités administratives, le secteur privé, le monde universitaire et la communauté internationale.

Dans le traitement de la cybersécurité au niveau national, les pouvoirs publics doivent jouer un rôle décisif en se préparant aux cyberincidents, en les détectant, en les gérant et en prenant des mesures afin d'y répondre. La mise en œuvre d'un mécanisme de gestion des incidents nécessite la prise en compte du financement, des ressources humaines, de la formation, des moyens techniques, des relations entre l'administration et le secteur privé et aussi des règles de droit. La collaboration à tous les niveaux de l'administration et avec le secteur privé, le monde universitaire et les organisations internationales est nécessaire pour harmoniser efficacement les moyens et les compétences permettant de gérer des incidents et de mieux faire connaître les incidents potentiels et les mesures à prendre en vue d'y remédier. L'administration a un rôle décisif à jouer pour assurer la coordination entre ces entités.

IV.A Aperçu des objectifs de cette partie

La mise en place, au niveau national, de structures de gestion des incidents nécessite l'exécution d'une série d'activités étroitement liées, à savoir:

IV.A.1 Mettre au point un système national coordonné de sécurité du cyberespace afin d'assurer la prévention, la prévision et la détection des incidents ainsi que les interventions et le retour à la normale.

IV.A.2 Désigner un coordonnateur chargé de gérer les cyberincidents afin de réunir les éléments critiques relevant des pouvoirs publics (y compris l'application des lois) et les éléments essentiels relevant des opérateurs et des fournisseurs d'infrastructures pour réduire à la fois les risques et la gravité des incidents.

IV.A.3 Participer aux mécanismes de partage d'informations concernant la surveillance, l'alerte et les interventions en cas d'incidents.

IV.A.4 Développer et tester des plans, des procédures et des protocoles d'intervention d'urgence pour veiller à ce que les collaborateurs des pouvoirs publics et autres puissent instaurer un climat de confiance et travailler efficacement de façon concertée en cas de crise.

IV.B Mesures spécifiques pour atteindre ces objectifs

La mise en place d'un potentiel national d'intervention en cas d'attaques du cyberespace est une entreprise à long terme qui commence par la création, au niveau national, d'une équipe de réponse aux incidents informatiques (CIRT).[12, 13]

IV.B.1 Identifier ou créer une structure nationale CIRT.

1. Réagir efficacement à un incident électronique majeur peut réduire les dommages causés aux systèmes d'information, procurer un moyen d'intervention efficace et réduire la durée et le coût du retour à la normale. Un centre CIRT désigné sur le plan national, conjointement avec les secteurs

---

[12] Voir la Résolution 58 de l'AMNT. Dans certains pays, on parle non pas de CIRT mais de centre national d'alerte et de réaction aux attaques informatiques (NCSIRT, National Computer Security Incidence Response Team ou N-SIRT, National Security Incident Response Team).

[13] Les résultats des travaux accomplis par l'UIT-T au titre de la Résolution 58 peuvent affecter la Partie IV des présentes bonnes pratiques.

public et privé, est nécessaire comme point de convergence au sein de l'administration, en particulier pour les incidents d'importance nationale, afin de coordonner la défense contre les cyberincidents et les mesures d'intervention à prévoir. Dans ces circonstances, les CIRT doivent travailler conjointement avec les autorités compétentes mais ne devraient ni diriger ni contrôler leurs activités.

2. On attend d'un CIRT qu'il fournisse des services et un soutien pour éviter les problèmes liés à la cybersécurité et y répondre. Il doit également servir de point de contact unique pour les comptes rendus, la coordination et les communications liés aux incidents de cybersécurité. La mission d'un CIRT devrait inclure l'analyse, l'alerte, le partage d'informations, la réduction de la vulnérabilité, les interventions ainsi que l'aide aux efforts nationaux de rétablissement des infrastructures essentielles de l'information. En particulier, un CIRT devrait remplir plusieurs fonctions au niveau national, consistant, notamment à:

- détecter et identifier une activité anormale;
- analyser les menaces et vulnérabilités électroniques et diffuser les informations d'alerte de menace électronique;
- analyser et synthétiser les informations sur les incidents et les vulnérabilités diffusées par d'autres, y compris les fournisseurs et les experts en technologie, afin de fournir une évaluation aux parties prenantes intéressées;
- établir entre les parties prenantes des mécanismes de communication de confiance et des communications de facilitation visant à partager l'information et à traiter les problèmes de cybersécurité;
- fournir des informations d'alerte rapide, dont des informations sur la réduction des vulnérabilités et les problèmes potentiels;
- développer des stratégies d'atténuation et d'intervention et réagir de façon coordonnée à l'incident;
- partager les données et les informations concernant l'incident et les interventions correspondantes;
- suivre et surveiller les informations pour déterminer les tendances et les stratégies de correction à long terme; et
- porter à la connaissance du public les bonnes pratiques générales pour la cybersécurité ainsi que des conseils pour faire face aux incidents et les prévenir.

IV.B.2 Instaurer au sein de l'administration un ou plusieurs mécanismes de coordination entre les organismes civils et publics.

1. Un CIRT a pour rôle fondamental de diffuser des informations aux parties prenantes intéressées, y compris des informations sur les vulnérabilités et menaces actuelles. Les parties prenantes qui doivent s'engager dans les activités d'intervention sont les organismes publics pertinents.

2. Une coordination efficace avec ces entités peut prendre diverses formes, par exemple: gérer un site web pour échanger des informations; fournir des informations via des listes d'adresses, y compris des bulletins, des rapports sur les tendances et les résultats d'études; produire des publications contenant alertes, conseils et informations sur divers aspects de la cybersécurité dont les nouvelles technologies, les vulnérabilités, les menaces et leurs conséquences.

IV.B.3 Etablir des relations de collaboration avec le secteur privé pour se préparer aux incidents électroniques nationaux, les détecter, y faire face et assurer le retour à la normale.

1. Les pouvoirs publics et le CIRT doivent collaborer avec le secteur privé. Sachant que, dans de nombreux pays, le secteur privé possède une bonne partie des infrastructures essentielles de l'information et des actifs des technologies de l'information, les pouvoirs publics et le secteur privé doivent collaborer pour atteindre l'objectif primordial qu'est la gestion efficace des incidents.

2. C'est grâce à des relations de collaboration avec le secteur privé, bâties sur la confiance, que les pouvoirs publics peuvent se familiariser avec une grande partie des infrastructures essentielles que

possède et exploite le secteur privé. La collaboration entre les secteurs publics et privés peut permettre de gérer les risques associés aux menaces, aux vulnérabilités électroniques et à leurs conséquences et développer une conscience situationnelle via le partage d'informations, l'ouverture et les engagements mutuels.

3. Encourager les pratiques de partage entre le secteur privé et les pouvoirs publics propres à faciliter le partage d'informations opérationnelles en temps réel.

4. Parmi les moyens d'encourager cette collaboration, on pourrait notamment en recenser les avantages pour l'administration et pour le secteur privé, développer et mettre en œuvre des programmes qui garantissent la protection de données privées sensibles, établir des groupes de travail secteur public/secteur privé sur la gestion des risques et la gestion des incidents électroniques, partager les bonnes pratiques permettant de gérer les incidents ou d'y faire face ainsi que les matériels de formation et, enfin, définir de façon concertée les rôles et les responsabilités de l'Etat et du secteur privé dans la gestion des incidents, l'objectif étant d'élaborer au fil du temps des protocoles cohérents et fiables.

IV.B.4 Instaurer un ou plusieurs points de contact au sein des organismes gouvernementaux, du secteur privé et des partenaires internationaux afin de faciliter la consultation, la coopération et l'échange d'informations avec le CIRT.

1. Un mécanisme – national ou international – d'intervention en cas d'incidents coordonné et efficace doit impérativement identifier les points de contact pertinents et établir des relations de travail pour la consultation, la coopération et l'échange d'informations. Ces relations peuvent encourager l'alerte rapide en cas d'incidents électroniques potentiels et l'échange d'informations sur les tendances, les menaces et les mesures à prendre par les entités chargées des interventions et autres parties prenantes.

2. Tenir à jour des points de contact et des canaux de communication avec les communautés des parties prenantes permet d'assurer des échanges d'information opportuns et proactifs à propos des tendances et menaces et d'accélérer les mesures d'intervention. Il est important d'établir, dans la mesure du possible, des contacts basés sur les fonctions d'un service plutôt que sur des personnes physiques, afin de s'assurer que les canaux de communication demeureront ouverts même après que les personnes physiques auront quitté l'organisation. Les relations débutent souvent par l'instauration d'un climat de confiance entre des personnes physiques particulières, mais elles devraient évoluer vers des arrangements institutionnels plus formels.

IV.B.5 Participer à des activités internationales de coopération et de partage d'informations.

1. L'administration doit encourager la collaboration avec les organisations, les fabricants et les autres experts appropriés spécialisés dans ce domaine pour: 1) faire reconnaître les dispositifs de réponse aux incidents comme une discipline à l'échelle internationale; 2) promouvoir et aider les CIRT à participer aux conférences et aux forums internationaux et régionaux existants afin de permettre d'améliorer les modes de réponse aux incidents actuels au niveau régional; et 3) participer au développement de supports pour mettre en place des CIRT nationaux et communiquer de manière efficace avec les autorités des CIRT.

IV.B.6 Développer des outils et des procédures pour la protection des ressources électroniques des entités gouvernementales.

1. La gestion efficace des incidents nécessite également le développement et la mise en œuvre de politiques, procédures, méthodologies, contrôles de sécurité et outils pour protéger les biens, systèmes, réseaux et fonctions électroniques des pouvoirs publics. Pour un CIRT, ceux-ci peuvent inclure des Procédures normalisées d'activité (PSA), des lignes directrices pour les activités internes et externes, des politiques de sécurité pour la coordination avec les parties prenantes, la mise en place de réseaux d'information sécurisés pour les activités du CIRT et des communications sécurisées. En tant que point de convergence pour les interventions en cas d'incidents, les CIRT devraient se coordonner entre eux et contribuer à rendre possible la collaboration avec d'autres entités chargées des interventions en cas d'incidents. Les gouvernements devraient par ailleurs dispenser aux personnels nouveaux et en place une formation continue dans ce domaine.

IV.B.7 Mettre en place par l'intermédiaire du CIRT, des moyens d'assurer la coordination des activités des pouvoirs publics afin de répondre aux cyberattaques de grande ampleur et d'assurer le retour à la normale.

1. En cas d'incident d'envergure nationale, il faudra prévoir un point central de contact pour assurer la coordination avec les autres organismes gouvernementaux ainsi qu'avec les autres communautés de partenaires comme le secteur privé. Il est important d'élaborer des plans et des procédures pour veiller à ce que le CIRT soit prêt à faire face à un incident possible.

IV.B.8 Encourager les pratiques de divulgation fiables pour protéger les activités et l'intégrité de l'infrastructure électronique.

1. Des vulnérabilités peuvent parfois être repérées dans des matériels informatiques ou des logiciels. Les décisions quant à leur divulgation au public devraient être prises au cas par cas, afin que les informations relatives à ces vulnérabilités ne soient pas utilisées de façon abusive. Les fournisseurs devraient être avertis suffisamment à l'avance en cas de divulgation de ces vulnérabilités.

PARTIE V

Promouvoir une culture nationale de la cybersécurité

Etant donné que les ordinateurs personnels deviennent toujours plus performants, que les technologies convergent, que l'utilisation des TIC se généralise et que les connexions transfrontières augmentent, toutes les parties prenantes qui développent, possèdent, fournissent, gèrent, entretiennent et utilisent des réseaux d'information doivent comprendre les questions de cybersécurité et prendre des mesures adaptées à leur rôle pour protéger les réseaux. Les pouvoirs publics doivent jouer un rôle pilote dans l'émergence de cette culture de la cybersécurité et dans l'appui aux efforts des autres parties prenantes.

V.A Aperçu de l'objectif de cette Partie

V.A.1 Promouvoir une culture nationale de la sécurité compatible avec les Résolutions 57/239, *Création d'une culture mondiale de la cybersécurité*[14] et 58/199, *Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information*[15] de l'Assemblée générale des Nations Unies.

1. La promotion d'une culture nationale de la sécurité ne traite pas uniquement du rôle des pouvoirs publics dans la sécurisation du fonctionnement et de l'utilisation des infrastructures de l'information, y compris les systèmes mis en œuvre par les pouvoirs publics, mais aussi de l'ouverture au secteur privé, à la société civile et aux particuliers. De la même façon, elle s'étend à la formation des utilisateurs des systèmes publics et privés, aux améliorations futures de la sécurité, et à d'autres questions importantes, dont le respect de la vie privée, les spams et les maliciels.

2. Selon l'OCDE, les moteurs clés d'une culture de la sécurité sur le plan national sont les applications et les services électroniques des pouvoirs publics ainsi que la protection des infrastructures nationales essentielles de l'information. Par conséquent, les administrations nationales devraient mettre en œuvre des applications et des services électroniques pour améliorer leurs activités en interne et fournir de meilleurs services au secteur privé et aux citoyens. Il conviendrait que la sécurité des systèmes et des réseaux d'information soit abordée non seulement dans une perspective technologique mais qu'elle tienne compte d'éléments comme la prévention et la gestion des risques et la sensibilisation de l'utilisateur. L'OCDE a constaté que l'impact bénéfique des activités de l'administration publique en ligne va au-delà des administrations publiques pour atteindre le secteur privé et les particuliers. Les initiatives dans le domaine de l'administration publique en ligne semblent avoir eu un effet multiplicateur, favorisant la diffusion d'une culture de la sécurité.

3. Les pays devraient adopter, par l'intermédiaire d'activités de collaboration, de préférence dans le cadre d'accords, une approche pluridisciplinaire et multi parties prenantes pour la mise en œuvre de la cybersécurité, certains instaurant d'ailleurs une structure de gouvernance de haut niveau pour la mise en œuvre des politiques nationales. Une plus grande sensibilisation et des initiatives pédagogiques sont considérées comme très importantes, de même que le partage de bonnes pratiques, la collaboration entre parties prenantes et l'utilisation de normes internationales.

4. La coopération internationale est extrêmement importante pour la promotion d'une culture de la sécurité, de même que le rôle des organismes régionaux, qui facilitent les interactions et les échanges.

V.B Mesures spécifiques pour atteindre cet objectif

V.B.1 Mettre en place un plan de sécurité pour les systèmes exploités par les pouvoirs publics.

1. La première étape d'une action des pouvoirs publics visant à sécuriser les systèmes qu'ils exploitent passe par le développement et la mise en place d'un plan de sécurité national. La préparation de ce

---

[14] www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf

[15] www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf

plan devrait aborder la gestion des risques, ainsi que la conception et la mise en œuvre de la sécurité. Le plan et sa mise en œuvre devraient être périodiquement réévalués afin d'en mesurer la progression et d'identifier les domaines dans lesquels ils doivent être améliorés. Le plan devrait également comprendre des dispositions au sujet de la gestion des incidents, y compris les mesures d'intervention, la veille, l'alerte, et le retour à la normale, ainsi que des liens pour l'échange d'informations. Le plan de sécurité devrait aussi comporter un volet formation des utilisateurs de ces systèmes publics qui est préconisé au point V.B.2 ainsi qu'une collaboration entre les pouvoirs publics, le secteur privé et la société civile en ce qui concerne la formation et les initiatives en matière de sécurité. La sensibilisation et la responsabilité de l'utilisateur sont les questions clés devant être traitées dans le cadre de la formation.

V.B.2 Lancer des programmes et des initiatives de sensibilisation à la sécurité destinés aux utilisateurs des systèmes et réseaux.

1. Pour être efficace, un programme national de sensibilisation à la cybersécurité devrait cibler à la fois le grand public et les principales communautés, tendre vers l'établissement de relations avec les professionnels gouvernementaux de la cybersécurité pour permettre le partage des informations sur les initiatives en matière de cybersécurité et vers l'instauration d'une collaboration en vue d'encourager la coopération sur les questions de cybersécurité. Lors de la mise au point d'un programme de sensibilisation, il y a trois éléments fonctionnels à prendre en considération: 1) les contacts avec les parties prenantes et l'engagement de celles-ci, l'objectif étant de nouer et de maintenir des relations de confiance entre le secteur privé, les pouvoirs publics et les milieux universitaires afin d'encourager la sensibilisation à la sécurité et sécuriser efficacement le cyberespace; 2) la coordination, dans le sens de l'établissement d'une collaboration entre les pouvoirs publics en ce qui concerne les manifestations et activités de cybersécurité; et 3) les communications et les messages privilégiant le développement de communications en interne (avec l'organisme gouvernemental responsable de ce programme) et les communications externes (autres organismes publics, industrie, établissements d'enseignement, utilisateurs d'ordinateurs privés et grand public).

V.B.3 Encourager le développement d'une culture de la sécurité dans les entreprises.

1. On peut développer une culture de la sécurité dans les entreprises de plusieurs façons innovantes. De nombreuses initiatives des pouvoirs publics ont été prises pour sensibiliser davantage les petites et moyennes entreprises (PME). Un dialogue entre les pouvoirs publics et les syndicats professionnels ou la collaboration entre les pouvoirs publics et le secteur privé peut aider les administrations à concevoir et à mettre en place des initiatives en matière d'éducation et de formation. Exemples de ce genre d'initiatives: diffuser l'information (hors ligne et en ligne), par exemple, brochures, manuels, modèles de politiques et de concepts; ouvrir des sites web spécialement destinés aux PME et à d'autres parties prenantes; dispenser une formation (en ligne); fournir un outil d'auto-évaluation en ligne; offrir des aides financières et fiscales ou autres visant à encourager la production de systèmes sécurisés ou prendre des mesures proactives afin de renforcer la cybersécurité.

V.B.4 Soutenir l'ouverture vers la société civile tout en accordant une attention particulière aux besoins des enfants, des jeunes, des personnes présentant des handicaps et des utilisateurs individuels.

1. Certains gouvernements ont coopéré avec le secteur privé pour sensibiliser davantage l'opinion aux nouvelles menaces et aux mesures qu'il faudrait prendre pour les contrer. Ils organisent des événements spécifiques, comme une journée, une semaine ou un mois de la sécurité de l'information, avec des activités organisées dans le but de promouvoir la sécurité de l'information auprès de nombreux destinataires, y compris du grand public. La plupart des initiatives visent à sensibiliser les enfants et les élèves par l'intermédiaire des professeurs et des parents, ou par la distribution directe de documents donnant des conseils. Les matériaux d'appui utilisés vont des sites web aux cartes postales, en passant par les jeux, les outils en ligne, les livres scolaires et les diplômes pour les examens passés. Comme exemples d'initiatives de ce genre, citons la fourniture de formations aux parents de jeunes enfants pour les informer des risques sécuritaires; la fourniture de matériel d'appui aux enseignants; la fourniture d'outils aux enfants pour jouer en ligne

parallèlement à la réception de messages éducatifs liés à la sécurité de l'information; la réalisation de livres scolaires et de jeux; la création d'un examen et d'un diplôme ainsi que d'un quiz sur la manière de surfer sur le web en toute sécurité.

2. Les pouvoirs publics et le secteur privé peuvent partager les leçons qu'ils ont apprises en développant des plans de sécurité et en formant des utilisateurs; tirer des enseignements des réussites et des innovations des autres; et travailler à améliorer la sécurité des infrastructures nationales de l'information.

V.B.5 Promouvoir un programme global national de sensibilisation afin que toutes les parties prenantes – les entreprises, la population active et le grand public – sécurisent leurs propres parts du cyberespace.

1. De nombreuses vulnérabilités des systèmes d'information sont dues à un manque de sensibilisation à la cybersécurité de la part des utilisateurs, des administrateurs de système, des développeurs, des responsables des achats, des auditeurs, des responsables des TI et des conseils d'administration. Ces vulnérabilités peuvent constituer un risque sérieux pour les infrastructures, même si elles ne font pas vraiment partie de l'infrastructure elle-même. La sensibilisation des administrateurs de système, par exemple, est souvent un maillon faible dans un plan de sécurité d'une entreprise. Promouvoir les efforts du secteur privé en matière de formation du personnel et répandre parmi les salariés la pratique d'une certification à la sécurité contribueront à la réduction de ces vulnérabilités. La coordination par les pouvoirs publics d'activités d'ouverture et de sensibilisation en faveur d'une culture de la sécurité renforcera par ailleurs la confiance du secteur privé. La cybersécurité est une responsabilité partagée. Les portails et les sites web peuvent constituer un mécanisme utile pour la promotion d'un programme national de sensibilisation, permettant aux organismes publics, aux entreprises et aux consommateurs individuels de prendre les mesures qui protégeront leurs portions de cyberespace.

V.B.6 Mettre en valeur les activités scientifiques et technologiques (S&T) et de recherche-développement (R&D).

1. Dans la mesure où les pouvoirs publics encouragent les activités dans les domaines de la science, de la technologie et de la recherche-développement, une partie de leurs efforts devrait être tournée vers la sécurité des infrastructures de l'information. A travers l'identification des priorités de la R&D dans l'électronique, les pays peuvent autant influencer le développement de produits à sécurité intégrée que faire face à de difficiles défis techniques. Dans la mesure où la R&D est menée au sein d'un établissement d'enseignement supérieur, il peut y avoir des occasions d'impliquer des étudiants dans des initiatives de cybersécurité.

V.B.7 Examiner le régime de respect de la vie privée existant et l'adapter à l'environnement en ligne.

1. Cet examen devrait tenir compte des dispositifs de respect de la vie privée adoptés par divers pays et par des organisations internationales comme l'OCDE. Les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, adoptées le 23 septembre 1980, constituent toujours le consensus international en matière de directive sur la collecte et la gestion d'informations à caractère personnel. En exposant des principes fondamentaux, les lignes directrices jouent un rôle majeur d'aide aux pouvoirs publics, aux représentants du monde des affaires et des consommateurs dans leurs efforts pour protéger la vie privée ainsi que les données à caractère personnel et pour remédier aux restrictions inutiles des flux de données transfrontières, à la fois en ligne et hors ligne.

V.B.8 Développer la connaissance des risques électroniques et des solutions disponibles.

1. Pour traiter des questions techniques il faut que les pouvoirs publics, les entreprises, la société civile et les utilisateurs individuels travaillent ensemble au développement et à la mise en place des mesures qui intègrent des éléments concernant la *technologie* (par exemple, des normes), les *processus* (par exemple, des lignes directrices volontaires ou des réglementations obligatoires) et le *personnel* (par exemple, de bonnes pratiques).

2. Un exemple de menace est le spam avec ses menaces connexes comme les maliciels. Plusieurs organisations, notamment la CE 17 de l'UIT-T, Question 4, étudient ces problèmes relatifs aux spams. L'Annexe A fournit une présentation détaillée de cette question.

3. La gestion d'identité est un exemple d'outil technologique visant à répondre aux différents besoins en matière de cybersécurité. Plusieurs organisations, notamment la CE 17 de l'UIT-T, Question 10, étudient la gestion d'identité. L'Annexe B fournit une présentation détaillée de cette question.

Appendice 1

Liste d'acronymes

APECTEL	*Asia-Pacific Economic Cooperation Telecommunications and Information Working Group*
CAN-SPAM	*Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003* (Etats-Unis)
CCIPS	*Computer Crime and Intellectual Property Section* (Ministère de la justice des Etats-Unis)
CERT	Equipe d'intervention en cas d'urgence informatique
CERT-CC	*Computer Emergency Response Team Coordination Center* (de la Carnegie Mellon University, Etats-Unis)
CII	Infrastructure essentielle de l'information
CIIP	Protection des infrastructures essentielles de l'information
CIRT	Equipe d'intervention en cas d'incident informatique
COE	Conseil de l'Europe
CPNI	*Centre for the Protection of National Infrastructure* (Royaume-Uni)
CSIRT	*Computer Security Incident Response Team* (centre d'alerte et de réaction aux attaques informatiques)
CVE	*Common Vulnerabilities and Exposures List* (Etats-Unis)
DHS	*Department of Homeland Security* (Etats-Unis)
DOJ	*Department of Justice* (Etats-Unis)
FAR	*Federal Acquisition Regulations* (Etats-Unis)
FCC	*Federal Communications Commission* (Etats-Unis)
FIRST	*Forum of Incident Response Security Teams*
G8	Groupe des Huit (Nations)
IMPACT	Partenariat multilatéral international contre les cybermenaces
ISAC	*Information Sharing and Analysis Center* (Centre d'échange et d'analyse des informations; divers, tel que IT-ISAC, Etats-Unis)
IT-ISAC	*Information Technology – Information Sharing and Analysis Center* (Centre d'échange et d'analyse des informations sur les technologies de l'information)
ITAA	*Information Technology Association of America*
LAP	*London Action Plan* (Plan d'action de Londres)
MSCM	*Mobile Service Commercial Message* (Message commercial pour les services mobiles)
NIAC	*National Information Assurance Council* (ITAA)
NIATEC	*National Information Assurance Training and Education Center* (Université d'Idaho, Etats-Unis)
NIST	*National Institute of Standards and Technology* (Etats-Unis)

NRIC	*Network Reliability and Interoperability Council* (FCC, Etats-Unis)
NSTAC	*National Security and Telecommunications Advisory Committee* (DHS, Etats-Unis)
NVD	*National Vulnerability Database* (Etats-Unis)
OCDE	Organisation de coopération et de développement économiques
OVAL	*Open Vulnerability Assessment Language* (langage commun pour la spécification des détails techniques des vulnérabilités et des problèmes de configurations)
PME	Petites et moyennes entreprises
PSTN	Réseau téléphonique public commuté
R&D	Recherche et développement
S&T	Science et technologie
SMS	Message court
SOP	Procédures d'exploitation normalisées
TCPA	*Telephone Consumer Protection Act* (Etats-Unis)
TIC	Technologies de l'information et de la communication
UE	Union européenne
UNGA	Assemblée générale des Nations Unies

Appendice 2

Stratégie de mise en oeuvre nationale pour la coopération en matière de cybersécurité et mesure de l'efficacité

L'approche indiquée plus haut repose sur une méthode de programme conçue pour amener les pays à mettre en place des systèmes de cybersécurité à titre de priorité nationale. Cette méthode comporte trois phases distinctes: évaluation initiale des capacités, mise en œuvre et évaluation du programme. Cette approche par étapes est exposée ci-dessous:

Méthode du programme de coopération en matière de cybersécurité et mesures de l'efficacité

Phase 1 – Analyser, évaluer et recommander un projet de programme d'échange fondé sur la coopération.

- **Analyser:** Un pays doit commencer par analyser son programme de sécurité actuel. Une équipe d'experts procède à cette analyse à l'aide d'un outil d'évaluation normalisé.
- **Evaluer:** Les informations rassemblées lors de cette analyse permettent de comprendre les forces et les faiblesses du programme de cybersécurité actuel du pays et de déterminer sur quoi les efforts devraient porter.
- **Recommander**: Les résultats de l'évaluation servent de base à l'élaboration d'un plan répondant aux besoins du pays.

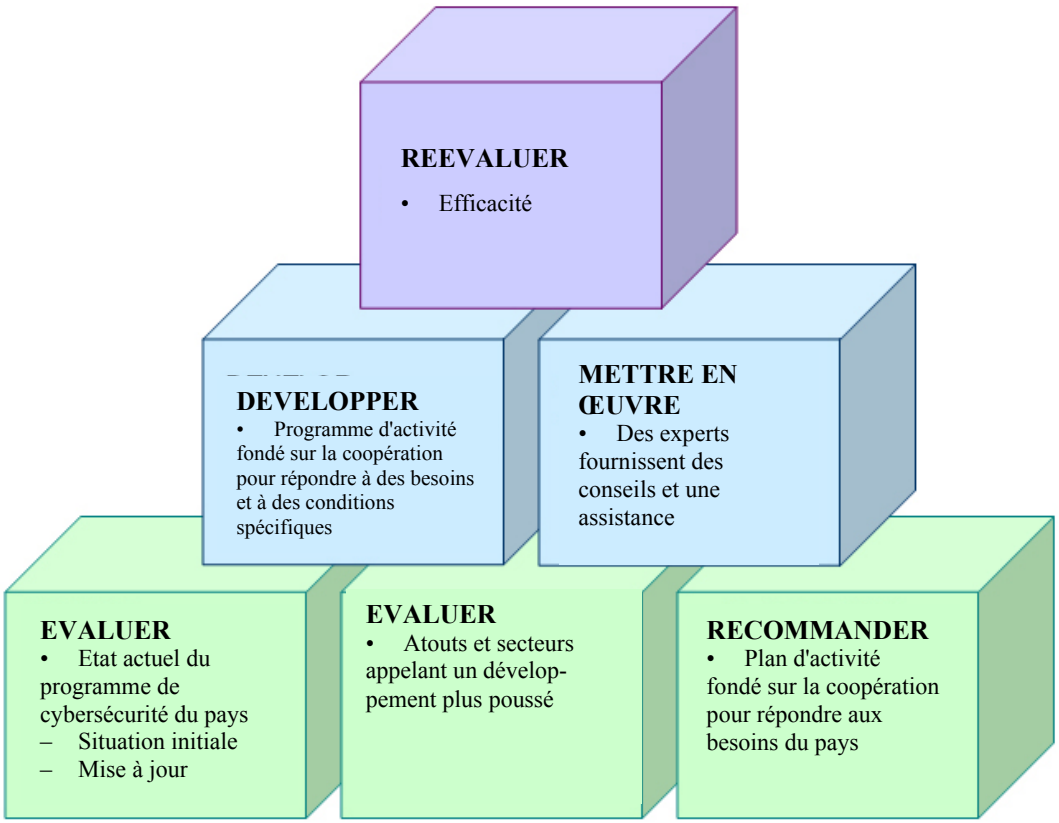
Phase 2 – Elaboration et mise en œuvre d'un programme fondé sur la coopération.

- **Elaboration d'un programme fondé sur la coopération:** Les experts du pays se rencontrent, ou se mettent en rapport avec des homologues internationaux pour concevoir, formuler et adapter les activités correspondant aux besoins et aux conditions spécifiques du pays considéré. Ces activités peuvent englober diverses activités d'échange axé sur la coopération et l'identification des besoins importants à long terme.
- **Programme de mise en œuvre:** Des experts nationaux et éventuellement internationaux mettent en place le programme et offrent des conseils pratiques.

Phase 3 – Evaluation du programme fondé sur la coopération afin d'évaluer le succès du programme et de le terminer.

- **Evaluation du programme fondé sur la coopération:** Périodiquement, le programme de cybersécurité est réévalué par rapport à son efficacité, en interne ou avec des homologues d'autres pays. Des domaines jugées insuffisants peuvent faire l'objet de nouveaux échanges de coopération et le processus précédent est relancé. Si un pays coopère avec d'autres, cette coopération peut prendre fin dès que le programme du pays est jugé efficace.

Figure 1: Méthodologie du programme de renforcement des capacités en matière de cybersécurité



On trouvera ci-après une approche permettant de mesurer la performance sur la durée dans ce domaine et d'expliquer les progrès réalisés à de hauts fonctionnaires. Il s'agit de construire une chaîne logique qui relie les entrées de base (programmes spécifiques à une région et/ou à un pays qui prennent du temps et nécessitent des ressources financières et de personnel) au résultat final recherché (une cybersécurité renforcée). Cette chaîne est illustrée par le tableau ci-après:

Catégorie de mesure:	**Elément de performance:**
Entrée de base:	**Programmes du pays:** • Temps • Argent • Personnel
Processus de travail de base:	**Travaux, comprenant éventuellement des échanges fondés sur la coopération, concernant:** • L'élaboration d'une stratégie nationale • L'élaboration du cadre juridique • La gestion des incidents • La collaboration pouvoirs publics/secteur privé • La culture de la cybersécurité

Résultats de base:

Nombre de:

- Réunions ou d'échange fondés sur la coopération
- Contacts avec de hauts fonctionnaires chargés des politiques et des aspects techniques

Résultats intermédiaires:

Mesures prises au niveau des pays:

- Nouvelles législations et réglementations sur la cybercriminalité
- Mesures visant à faire respecter les lois
- Création d'un CSIRT
- Programmes de sensibilisation pouvoirs publics/secteur privé
- Demandes de renseignements sur les interventions en cas d'incident
- Participation à des activités d'organisations internationales dans le domaine de la cybersécurité
- Adhésion à des conventions et à des lignes directrices internationales

Résultat final: Réduction des risques de cybersécurité grâce à un cadre juridique et politique national, des moyens de réaction aux incidents informatiques et des initiatives de sensibilisation.

Résultat définitif: Amélioration de la cybersécurité nationale et de la sécurité au niveau mondial.

Annexe A

Etude de cas: le spam

UNION INTERNATIONALE DES TELECOMMUNICATIONS

UIT-T

SECTEUR DE
NORMALISATION DES
TÉLÉCOMMUNICATIONS
DE L'UIT

Série X

Supplément 6
(09/2009)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Série UIT-T X.1240 – Supplément sur la lutte contre le spam et les menaces associées

ATTENTION !
RECOMMANDATION PRÉPUBLIÉE

Ce texte est la version non éditée d'une Recommandation approuvée récemment. Il sera remplacé par la version finale après édition. Certaines différences peuvent donc apparaître entre ce texte et sa version éditée finale.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (TIC). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIETE INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous www.itu.int/ITU-T/ipr/.

Supplément 6 aux Recommandations UIT-T de la série X

Série UIT-T X.1240 – Supplément sur la lutte contre le spam et les menaces associées

Résumé

Le Supplément 6 aux Recommandations UIT-T de la série X indique que pour lutter efficacement contre le spam, les pouvoirs publics doivent recourir à différentes méthodes comprenant notamment des législations efficaces et des outils technologiques et la sensibilisation des consommateurs et des entreprises. Le présent Supplément passe en revue les instances internationales qui examinent le problème du spam. En tant qu'étude de cas, il fournit à titre d'exemple des renseignements sur les méthodes adoptées par les Etats-Unis et le Japon pour faire face au problème du spam.

Source

Le Supplément 6 aux Recommandations UIT-T de la série X a été approuvé le 25 septembre 2009 par la Commission d'études 17 de l'UIT-T (2009-2012).

TABLE DES MATIERE

Supplément 6 aux Recommandations l'UIT-T de la Série X

Série UIT-T X.1240 – Supplément sur la lutte contre le spam et les menaces associées

1 Domaine d'application

Le présent Supplément traite du spam et des menaces associées. Il s'adresse aux administrateurs nationaux qui ne connaissent pas très bien le problème du spam et souhaitent obtenir des informations générales sur ce sujet.

Le présent Supplément traite des outils à utiliser pour lutter efficacement contre le spam et décrit les travaux accomplis par certaines instances internationales dans ce domaine. Il fournit, sous la forme d'une étude de cas et à des fins illustratives, une description des moyens mis en œuvre aux Etats-Unis et au Japon pour lutter contre le spam.

2 Références

Néant.

3 Définitions

Le présent Supplément définit les termes suivants:

3.1 **hameçonnage** (phishing): tentative visant à induire en erreur une personne en la dirigeant vers un site web erroné dans l'intention de lui subtiliser des données privées.

3.2 **spam**: bien qu'aucune définition du spam n'ait été adoptée à l'échelle mondiale, ce terme est couramment employé pour décrire des communications électroniques de masse non sollicitées transmises par courrier électronique (courriel) ou par messagerie mobile (SMS, MMS).

4 Abréviations et acronymes

Le présent Supplément utilise les abréviations suivantes:

ADSP	Author Domain Signing Practices
APEC TEL	Asia-Pacific Economic Cooperation – Telecommunications & Information Working Group (Coopération économique Asie-Pacifique – Groupe de travail sur les télécommunications et l'information)
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act (Loi sur la lutte contre la prolifération de la pornographie et des publicités non sollicitées) de 2003 (Etats-Unis)
CNSA	Contact Network of Spam Authorities (Réseau de contact des autorités antispam de l'Union européenne)
DKIM	DomainKeys Identified Mail (courrier identifié par clés de domaine)
FAI	Fournisseur d'accès à l'Internet
FCC	Federal Communications Commission (Commission fédérale des communications des Etats-Unis)
FTC	Federal Trade Commission (Commission fédérale du commerce des Etats-Unis)

JEAG	Japan Email Anti-abuse Group (Groupe contre l'utilisation abusive du courrier électronique au Japon)
LAP	Plan d'action de Londres (London Action Plan)
MAAWG	Groupe de travail contre l'utilisation abusive des messageries (Messaging Anti-Abuse Working Group)
MMS	Service de messagerie multimédia
MSCM	Messages commerciaux pour les services mobiles (Mobile Service Commercial Messages)
OCDE	Organisation de coopération et de développement économiques
OP25B	Outbound Port 25 Blocking (blocage du port 25 en sortie)
SMS	Service de messages courts (Short Message Service)
SPF	Sender Policy Framework

5 Conventions

Néant.

6 Généralités

6.1 **Le spam** est passé du stade de message publicitaire gênant à celui de source de problèmes de sécurité plus importants sur l'Internet. Par exemple, il peut être un moyen de tromperie permettant de diffuser des maliciels, comme les virus ou les logiciels espions, et d'inciter les consommateurs à fournir des informations confidentielles à des fins d'usurpation d'identité (hameçonnage). Les expéditeurs de spam profitent du fait qu'ils peuvent envoyer leurs messages depuis n'importe où et à n'importe qui dans le monde à un coût extrêmement faible, faisant du spam un problème international qui doit être traité dans le contexte d'une coopération internationale.

6.2 **Le hameçonnage** profite du fait que, en raison d'une caractéristique de base du système de messagerie électronique par Internet[16], toute personne peut envoyer un courriel à toute autre personne sans pratiquement aucune forme d'authentification. Le hameçonnage est une tentative visant à tromper une personne en la dirigeant vers un site web erroné dans l'intention de lui subtiliser des données privées. Le phénomène s'explique en grande partie par le fait qu'il arrive que certaines personnes s'attendent à recevoir du courrier électronique d'un site connu et ne se rendent tout simplement pas compte que le courriel reçu ne provient pas du bon site. Comme l'authentification n'existe guère dans le courrier électronique, il est difficile de déterminer si un message est authentique sans l'inspecter soigneusement. Cette inspection minutieuse exige une connaissance approfondie des mécanismes sous-jacents utilisés sur le web.

Le hameçonnage existe aussi parce qu'il est difficile pour la plupart des utilisateurs de vérifier que les sites web qu'ils visitent sont authentiques. Il arrive parfois que l'on oublie d'examiner de près l'adresse URL d'une page web avant d'introduire des informations confidentielles ou que l'on ne sache pas exactement quelle devrait être l'adresse URL correcte.

Par ailleurs, les serveurs web utilisés pour "hameçonner" les informations confidentielles sont souvent eux-mêmes victimes de maliciels, de sorte qu'il est encore une fois extrêmement difficile de suivre la trace des hameçonneurs.

---

[16] Le système de courrier électronique sur l'Internet a été conçu dans les années 70 lorsque l'accès à l'Internet était limité à quelques chercheurs et membres du gouvernement. Étant donné l'absence de besoin d'authentification de l'identité des expéditeurs de courrier électronique, aucun effort n'a été fait pour concevoir le système de façon à permettre cette authentification. S'il est vrai que le système de courrier électronique a évolué depuis, cette omission fondamentale subsiste encore.

6.3 **Les maliciels** ou logiciels malveillants, qui fonctionnent sur un ordinateur à l'insu ou sans la permission du propriétaire, posent également un problème important.

7 Approches à adopter au niveau national pour lutter efficacement contre le spam et menaces associées

7.1 **Stratégie nationale et spam.** En matière de stratégie nationale, les pays devraient mettre en place et appliquer une législation efficace, des autorités et des outils pour l'application des lois ainsi que des outils et de bonnes pratiques technologiques, et sensibiliser les consommateurs et les entreprises pour faire face efficacement au spam.

7.2 **Cadres juridique et réglementaire et spam.** S'agissant des cadres juridiques et réglementaires, les autorités compétentes en matière de spam doivent être habilitées à enquêter sur les infractions aux lois relatives au spam commises depuis leur pays ou produisant des effets dans leur pays et à prendre des mesures contre ces infractions. Ces autorités devraient par ailleurs définir de mécanismes de coopération avec les autorités étrangères. Les demandes d'assistance provenant des autorités étrangères devraient être classées par ordre de priorité en fonction des éventuels domaines d'intérêt commun et selon la gravité des infractions.

7.3 **Collaboration entre les pouvoirs publics et le secteur privé et encouragement à la sensibilisation nationale au problème du spam et aux menaces associées.** Toutes les parties prenantes, y compris les autorités chargées de faire respecter la législation, les entreprises, les associations du secteur privé et les associations de consommateurs, devraient coopérer dans la lutte contre les infractions à la législation se rapportant au spam. Les organismes gouvernementaux chargés de faire respecter la loi devraient collaborer avec les associations d'entreprises et les associations de consommateurs afin de sensibiliser les utilisateurs et d'encourager le partage des informations. Ils devraient également coopérer avec le secteur privé afin d'encourager l'élaboration d'outils technologiques destinés à lutter contre le spam, y compris des outils destinés à faciliter la localisation et l'identification des spammeurs.

Le délit de hameçonnage est souvent évitable. Les pouvoirs publics devraient collaborer avec le secteur privé afin d'améliorer les moyens de protéger les citoyens contre ce délit et de sensibiliser les consommateurs et les entreprises aux méthodes d'authentification sécurisées.

Les pouvoirs publics peuvent jouer un rôle en sensibilisant le public à la nécessité de lutter contre les maliciels par l'utilisation d'outils tels que les logiciels antivirus et des programmes de correction et des techniques informatiques éprouvées les plus récents.

8 Initiatives internationales (multilatérales) de lutte contre le spam

Plusieurs forums multilatéraux travaillent actuellement sur des initiatives de lutte contre le spam, à savoir:

8.1 Le Plan d'action de Londres

La Federal Trade Commission (FTC) des Etats-Unis et l'Office of Fair Trading du Royaume-Uni ont organisé à Londres, en 2004, une Conférence internationale sur l'application des lois antispam qui a conduit à l'élaboration du Plan d'action de Londres (LAP) sur la coopération internationale relative à l'application des lois antispam. En juillet 2008, des organismes gouvernementaux et des représentants du secteur privé de plus de 25 pays avaient adhéré au Plan. Le LAP encourage les parties intéressées, notamment les organismes chargés de faire respecter les lois antispam et les partenaires du secteur privé, à envisager de devenir membres de l'organisation.

Le but du LAP est de favoriser la coopération internationale pour l'application des lois antispam et de traiter les questions relatives au spam, comme l'abus de confiance et la tromperie, le hameçonnage et la diffusion de virus. Le LAP établit des relations entre ces entités à partir d'un document concis qui indique un plan de travail de base visant à améliorer, au niveau international, le respect des lois et la coopération aux fins de la sensibilisation contre les messages de spam illégaux. Ce document n'est pas contraignant, les participants étant seulement invités à faire tout leur possible pour mettre en œuvre le plan de travail (londonactionplan.org/).

Depuis sa création, le LAP a organisé des ateliers annuels, généralement en collaboration avec le Réseau de contact des autorités antispam (CNSA) de l'Union européenne. En octobre 2007, le LAP et le CNSA ont organisé leur atelier annuel commun en parallèle avec le Groupe de travail contre l'utilisation abusive des messageries (MAAWG), à Arlington (Virginie), ce qui a facilité le renforcement de la coopération avec le secteur privé en matière d'application des lois. En octobre 2008, le LAP et le CNSA ont organisé leur atelier annuel commun en parallèle avec le 6e Sommet allemand antispam organisé à Wiesbaden (Allemagne).

8.2 Boîte à outils antispam de l'OCDE et Recommandation du Conseil de l'OCDE relative à la coopération dans l'application des législations contre le spam

En avril 2006, le Groupe de réflexion sur le spam de l'OCDE a publié une "Boîte à outils" antispam, qui contient des recommandations visant à aider les décideurs, les régulateurs et les acteurs du secteur privé à orienter leurs politiques concernant les mesures contre le spam ainsi qu'à restaurer la confiance dans l'Internet et dans les courriels. La Boîte à outils comprend huit éléments, dont la réglementation antispam, les initiatives antispam du secteur privé et les technologies antispam, l'information et la sensibilisation ainsi que la coopération/l'ouverture au niveau mondial. Reconnaissant que la coopération internationale est cruciale pour lutter contre le spam, les gouvernements de l'OCDE ont également approuvé une "Recommandation relative à la coopération transfrontière dans l'application des législations contre le spam", qui invite instamment les pays à faire en sorte que leurs législations permettent aux autorités chargées de les faire appliquer de partager les informations avec d'autres pays et qu'elles le fassent de façon plus rapide et plus efficace (www.oecd-antispam.org/sommaire.php3).

8.3 Colloque de l'APEC TEL sur le spam

En avril 2006, l'APEC TEL a tenu un colloque sur "Le spam et les menaces connexes" qui a rassemblé trente orateurs et invités, afin d'étudier l'évolution du problème du spam et d'élaborer un calendrier commun d'action pour le TEL. Les principaux sujets suivants ont été abordés:

1) la mise en place et l'application de régimes de réglementation nationaux antispam, dont des mesures d'application et des codes de pratique;
2) le rôle du secteur privé dans la lutte contre le spam, y compris la collaboration entre les pouvoirs publics et l'industrie;
3) les réponses techniques au spam;
4) la coopération transfrontière et la mise en application des législations, dont la Convention sur la cybercriminalité du Conseil de l'Europe et la Recommandation du Conseil de l'OCDE relative à la coopération dans l'application des lois, comme principaux outils pour renforcer la coopération; et
5) les besoins croissants d'informations et de sensibilisation ciblées sur le consommateur.

Principales mesures concrètes que le TEL a décidé d'appliquer dans l'avenir:

1) encourager le partage des informations relatives à la réglementation et aux politiques, en utilisant des ressources telles que la Boîte à outils antispam de l'OCDE;
2) établir une liste de contacts pour les autorités antispam à ajouter aux ressources analogues créées par l'OCDE et par l'UIT;
3) encourager les pays à participer à des forums de coopération volontaire comme le Plan d'action de Londres ou le Mémorandum d'accord Séoul-Melbourne;
4) coopérer avec l'OCDE en matière de partage de l'information et d'orientation; et
5) appuyer le renforcement des capacités des pays en développement à faire face au spam.

9 Etude de cas sur certaines activités de lutte contre le spam

Dans cette section, on présente les activités menées dans certains pays pour lutter contre le spam.

9.1 Etats-Unis

9.1.1 Lois définissant les règles applicables aux diffuseurs de courriels commerciaux (CAN-SPAM Act)

En 2003, les Etats-Unis ont promulgué le "CAN-SPAM Act", qui fixe les règles applicables aux *diffuseurs de courriels commerciaux, explique clairement les sanctions applicables aux émetteurs de* spams et aux entreprises dont les produits font l'objet d'une publicité par spam s'ils enfreignent la loi, et donne aux consommateurs le droit de demander aux émetteurs de courriels de cesser de leur envoyer des spams.

Les principales dispositions du CAN-SPAM Act sont notamment les suivantes:

- **Les en-têtes de message faux ou trompeurs sont interdits**. Les "De", "A" des courriels, ainsi que les renseignements sur leur itinéraire, y compris le nom de domaine de départ et l'adresse de messagerie, doivent être exacts et identifier l'auteur du courriel.
- **Les lignes objet trompeuses sont interdites**. La ligne objet ne doit pas tromper le destinataire quant au contenu ou à l'objet du message.
- **Les courriels doivent donner aux destinataires une possibilité d'exemption (opt-out)**. L'expéditeur doit fournir une adresse de messagerie électronique pour la réponse ou un autre système de réponse par Internet qui permette au destinataire de demander la cessation de l'envoi de courriels à cette adresse, et ces demandes doivent être respectées. L'expéditeur peut proposer un "menu" de choix pour permettre au destinataire de refuser certaines sortes de messages, mais doit inclure l'option de cesser tout envoi de message commercial de la part de cet expéditeur. Tout mécanisme de refus d'envoi proposé par l'expéditeur doit permettre de traiter les demandes de refus d'envoi pendant au moins 30 jours après l'envoi du courriel en question. Sur réception d'une demande de refus de courriel, la loi donne 10 jours ouvrables à l'expéditeur pour cesser d'envoyer des courriels à l'adresse Internet du demandeur. L'expéditeur ne doit ni aider une autre entité à envoyer des courriels à cette adresse, ni faire envoyer de courriels en son nom à cette adresse par une autre entité. Enfin, l'expéditeur n'a pas le droit de vendre ou de transférer les adresses de courrier électronique de personnes qui choisissent de ne pas recevoir ses courriels, même sous la forme d'une liste d'adresses, à moins qu'il ne transfère ces adresses de telle manière que l'autre entité puisse respecter la loi.
- **Les courriels commerciaux doivent être identifiés en tant que publicités et doivent inclure l'adresse physique postale valable de l'expéditeur**. Les messages doivent contenir l'indication claire et visible qu'il s'agit de publicités ou de sollicitations et que le destinataire peut choisir de ne plus recevoir de courriel commercial de la part de leur expéditeur. Ils doivent aussi inclure l'adresse physique postale valable de celui-ci.

La Federal Trade Commission (FTC) des Etats-Unis est habilitée à exercer son pouvoir d'exécution des dispositions du Code civil pour faire respecter le CAN-SPAM Act et à infliger des amendes administratives pouvant atteindre 11 000 USD par infraction. Depuis que la FTC a pris sa première mesure d'application visant les messages commerciaux non sollicités (spams) en 1997, elle a engagé 94 actions en justice pour lutter contre les pratiques trompeuses et déloyales en matière de spam, dont 31 à l'encontre d'émetteurs de spam ayant enfreint le CAN-SPAM Act.

Le CAN-SPAM autorise par ailleurs le Ministère de la justice à faire appliquer ses sanctions pénales. Le CAN-SPAM Act prévoit des sanctions pénales importantes, y compris des peines de prison pour les émetteurs de spam. D'autres organismes fédéraux et organismes d'Etat peuvent opposer cette loi à des organisations selon leurs compétences, et les entreprises qui fournissent un accès Internet peuvent également poursuivre les auteurs d'infractions.

9.1.2 Lois interdisant l'envoi de courriels commerciaux aux appareils sans fil

Les Etats-Unis ont en outre adopté une réglementation visant à protéger les consommateurs contre la réception de messages commerciaux non sollicités (spam) sur leurs appareils sans fil. A quelques exceptions près, ces règles interdisent l'envoi de messages électroniques commerciaux, y compris les courriels et certains messages textuels, aux appareils sans fil, comme les téléphones portables. Ces dispositions ne s'appliquent qu'aux messages correspondant à la définition du mot "commercial" utilisée dans le CAN-

SPAM Act, ainsi qu'aux messages dont le principal but est de faire la publicité commerciale ou la promotion d'un produit ou d'un service commercial. Les messages non commerciaux, tels que les messages concernant des candidats à une fonction élective ou les messages destinés à mettre à jour le compte d'un client existant, ne sont pas soumis à ces règles.

Les messages commerciaux pour les services mobiles (MSCM) comprennent tout message commercial envoyé à une adresse de courrier électronique attribuée par un fournisseur de services mobiles à l'appareil sans fil d'un abonné. Les MSCM sont interdits sauf autorisation expresse donnée à l'expéditeur par le destinataire individuel (condition connue sous le nom de "*opt-in*"). La réglementation interdit d'envoyer quelque message commercial que ce soit à des adresses qui contiennent des noms de domaine inscrits sur la liste de la FCC depuis au moins 30 jours ou avant ces 30 jours si l'expéditeur sait par ailleurs que le message est adressé à un appareil sans fil. Afin d'aider les expéditeurs de messages commerciaux à identifier les adresses qui appartiennent à des abonnés au téléphone sans fil, la réglementation exige que les entreprises de télécommunications mobiles procurent à la *Federal Communications Commission* (FCC) les noms de domaine du courrier concerné. Les messages courts (SMS) qui ne sont transmis qu'à des numéros de téléphone ne sont pas couverts par ces protections. Les appels composés automatiquement sont déjà couverts par d'autres lois.

Selon la réglementation de la FCC, la FCC peut imposer aux expéditeurs de spam des saisies financières d'un montant pouvant aller jusqu'à 11 000,00 USD par infraction pour les personnes non autorisées et jusqu'à 130 000,00 USD par infraction pour un opérateur réseau grande distance autorisé. En plus des sanctions financières, la FCC peut prendre une ordonnance de cessation et d'abstention à l'encontre d'un expéditeur de spam qui a enfreint une disposition du *Communications Act* ou une disposition de la FCC autorisée par le *Communications Act*. En outre, selon ce *Communications Act*, toute personne contrevenant à une disposition de l'Act est passible de poursuites pénales de la part du Ministère de la justice (en plus d'une sanction financière), et risque jusqu'à un an d'emprisonnement (jusqu'à deux ans pour les récidivistes). A ce jour, la FCC n'a pas encore engagé de poursuites visant à faire respecter la loi concernant ce genre de messages commerciaux.

9.1.3 Méthodes visant à limiter le hameçonnage

Comme indiqué plus haut, les spammeurs et les hameçonneurs partent du principe que les données concernant l'expéditeur du courrier électronique font défaut. Le Groupe d'étude sur l'ingénierie Internet a publié deux normes, DomainKeys Identified Mail (DKIM) [b-IETF RFC 4871] et Author Domain Sending Practices (ADSP) [b-IETF RFC 5617], qui offrent au destinataire de meilleures possibilités d'identifier l'expéditeur. Les fabricants ont commencé à mettre certaines versions de la norme à la disposition des clients. Par ailleurs, il existe au moins une application gratuite[17] de la norme. On pourra trouver une aide auprès du *Anti-Phishing Working Group* (APWG), association d'acteurs du marché qui vise à éliminer l'usurpation d'identité et les escroqueries imputables au problème croissant que constituent le hameçonnage et la mystification par courrier électronique. L'organisation constitue un forum de discussions des questions de hameçonnage. Elle teste et évalue par ailleurs les solutions technologiques potentielles et offre un accès à une banque de données centralisée répertoriant les incidents de hameçonnage (www.antiphishing.org).

Ces normes permettent une "validation par signature" ou offrent aux utilisateurs la possibilité de vérifier, par exemple, que ce sont bien leur banque, leurs amis ou leurs associés qui cherchent à prendre contact avec eux. Ces normes en elles-mêmes permettront de limiter certains types de hameçonnage, mais pas tous.

9.2 Japon

9.2.1 Application de la législation

Il existe deux lois visant à limiter les envois de courriels en vue de lutter contre le spam au Japon. Les principales dispositions de ces lois sont présentées ci-dessous.

---

[17] Le terme "gratuit" signifie ici la possibilité d'appliquer cette norme sans redevances, aux conditions prescrites par le titulaire du brevet.

– Les dispositions suivantes s'appliquent à l'envoi de messages publicitaires par courrier électronique ("Opt-in", formule d'acceptation expresse):
  • L'envoi de messages publicitaires par courrier électronique sans le consentement du destinataire est interdit.
  • L'entité expéditrice est tenue de conserver des preuves du consentement des destinataires lorsqu'elle leur envoie des messages publicitaires.
  • Les messages publicitaires doivent comporter des informations sur la procédure à suivre pour demander la cessation de l'envoi de tels messages, notamment le nom de l'expéditeur.
  • Si un destinataire applique dûment la procédure prévue pour informer l'entité expéditrice qu'il ne souhaite pas recevoir de messages publicitaires, l'entité expéditrice ne peut plus envoyer de messages publicitaires à ce destinataire.
– L'envoi de courriers électroniques comportant de fausses informations sur l'expéditeur, notamment l'adresse de courrier électronique, l'adresse IP et le nom de domaine, est interdit.
– L'envoi de courriers électroniques à des adresses de destinataires fictives générées automatiquement par un programme informatique est interdit.

9.2.2 Conseil pour la promotion des mesures antispam

Diverses parties prenantes, notamment des FAI, des agences de publicité, des fournisseurs de services d'application proposant des services de courrier électronique publicitaire, des fournisseurs de logiciels de sécurité informatique, des organisations de consommateurs et des administrations, ont mis sur pied en 2008 le Conseil pour la promotion des mesures antispam. Celui-ci a adopté une Déclaration pour l'élimination du spam en novembre 2008.

9.2.3 Le *Cyber Clean Center*

Le *Cyber Clean Center* (CCC), qui a pour mission de rechercher les PC contaminés par des botnets, est le fruit d'une collaboration étroite entre le Gouvernement japonais, des organismes rattachés aux FAI et les principaux "FAI". Le Centre fonctionne de la façon suivante:
– Le CCC gère un réseau "leurre" à grande échelle ayant pour fonction de recevoir les communications de PC contaminés par des maliciels (généralement des botnets) destinées à propager la contamination. Ce réseau leurre relève l'adresse IP des PC contaminés ainsi que les codes des programmes des maliciels (ou botnets).
– Le CCC envoie les listes d'adresses IP, y compris la date/l'heure à laquelle elles ont été relevées, à chaque FAI concerné. Ceux-ci identifient leurs abonnés concernés au moyen de ces adresses IP et les informent que leur PC est peut-être contaminé par des logiciels malveillants. Les FAI fournissent également à ces abonnés des renseignements sur le CCC (notamment l'adresse du site web de celui-ci) et sur des logiciels d'élimination des virus.
– Le CCC analyse les codes de programmes recueillis. Si un code est identifié pour la première fois, un nouveau logiciel capable de protéger contre ce nouveau programme malveillant est mis au point et rendu disponible.

Ces travaux contribuent à réduire les activités de contamination des botnets au Japon. Etant donné que la plupart des spams sont envoyés par des PC contaminés par des botnets, cette réduction contribue également à faire diminuer le nombre de spams provenant du Japon.

9.2.4 Blocage du port 25 en sortie (OP25B – *Outbound Port 25 Blocking*)

Lorsqu'ils envoient ou reçoivent des courriels, les abonnés d'un FAI utilisent un service de courrier électronique généralement fourni par le FAI. Les abonnés envoient leurs courriels aux serveurs de courrier électronique du FAI, qui les transmettent aux serveurs de destination. Les abonnés n'envoient généralement pas leurs messages directement aux serveurs de courrier électronique de destination. Les PC contaminés par des botnets ou par des virus envoient des spams directement aux serveurs de courrier électronique de l'adresse de destination, de sorte que ces spams ne passent pas par les serveurs de courrier électronique des FAI. Si les communications des PC des abonnés qui contournent le réseau des FAI en utilisant le protocole de transfert de messages en mode simple (SMTP, correspondant au protocole de commande de transmission (TCP) avec le port 25) peuvent être arrêtées, de nombreux spams peuvent être bloqués. En conséquence, le

Gouvernement japonais, les FAI et les autres organismes concernés ont collaboré étroitement afin d'examiner les questions suivantes:

– incidences sur les abonnés du blocage du TCP sur le port 25 en sortie (OP25B) [b-MAAWG MP25];

– restrictions applicables au blocage de certaines communications en vertu de la législation japonaise actuelle.

Suite à l'examen de ces questions, de nombreux FAI appliquent désormais la méthode OP25B. Le JEAG (Groupe contre l'utilisation abusive des e-mails au Japon) a joué un rôle important dans cette évolution en publiant une recommandation exhortant vivement les FAI à appliquer la méthode OP25B.

– Bien que la méthode OP25B ne soit pas obligatoire pour les FAI japonais, 52 d'entre eux, y compris la plupart des plus grands FAI, l'avaient adoptée en juillet 2009.

– De nombreux FAI ayant adopté la méthode OP25B fournissent le service d'authentification SMTP AUTH utilisant le port 587 du protocole TCP, afin de proposer un autre moyen de communication de façon à maintenir la qualité de service. Les utilisateurs peuvent envoyer au serveur de ces FAI des messages provenant des serveurs d'autres FAI appliquant la méthode OP25B.

9.2.5 Technologies d'authentification de l'expéditeur

Les technologies d'authentification de l'expéditeur sont des techniques permettant de détecter la simulation des adresses sources dans les courriels. Le JEAG a publié une recommandation visant à encourager l'adoption de ces techniques, et le Ministère des affaires intérieures et de la communication a publié un document sur les questions juridiques importantes relatives à l'introduction par un FAI de l'authentification de l'expéditeur par le récepteur. Actuellement, presque tous les plus grands opérateurs mobiles et certains FAI ont adopté le SPF (*Sender Policy Framework*) [b-IETF RFC 4408], l'une des technologies existantes pour l'authentification de l'expéditeur, et leurs abonnés peuvent utiliser les résultats de l'authentification à des fins de filtrage. Le taux d'entrées SPF ("SPF records") publiées pour des domaines "jp" était de 35,99% en août 2009. En outre, plusieurs FAI ont commencé à appliquer la norme DKIM [b-IETF RFC 4871] comme mesure supplémentaire pour l'authentification de l'expéditeur.

9.2.6 Echange d'informations sur les expéditeurs de spam entre opérateurs mobiles

Au Japon, presque tous les téléphones mobiles prennent en charge le courrier électronique ordinaire. Etant donné que, dans ce pays, de nombreux spams sont envoyés depuis des téléphones mobiles, tous les opérateurs mobiles échangent des informations sur les expéditeurs de spams en appliquant les mesures suivantes:

– L'identité de toute personne souhaitant conclure un contrat de téléphonie mobile est vérifiée en vertu du "*Mobile Phone Improper Use Prevention Act*" (loi sur la prévention de la mauvaise utilisation des téléphones mobiles).

– Lorsqu'un opérateur mobile découvre qu'un utilisateur de téléphone mobile envoie des spams et enfreint l'"*Act on Regulation of Transmission of Specified Electronic Mail*" (loi sur la réglementation de la transmission de certaines formes de courrier électronique), il communique les données concernant cet utilisateur à tous les autres opérateurs mobiles.

Un utilisateur ayant envoyé des spams depuis un téléphone mobile aura donc des difficultés à conclure d'autres contrats d'utilisation de téléphones mobiles au Japon.

Une organisation à but non lucratif associée met en place des détecteurs, recueille les spams et les analyse. Elle fournit des informations sur les expéditeurs de spams aux FAI de ces expéditeurs et échange ces informations avec certains organismes à l'étranger.

Bibliographie

b-IETF RFC 4871] IETF RFC 4871 (2007), *Domainkeys Identified Mail (DKIM) Signatures.* www.ietf.org/rfc/rfc4871.txt

[b-IETF RFC 5617] IETF RFC 5617 (2009), *Domainkeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP).* www.ietf.org/rfc/rfc5617.txt

[b-MAAWG MP25] Recommandation du MAAWG (2005), *Gestion du port 25 dans l'espace IP dynamique ou résidentiel: avantages liés à l'adoption et risques liés à l'inaction.* www.maawg.org/port25

[b-IETF RFC 4408] IETF RFC 4408 (2007), *Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1.* www.ietf.org/rfc/rfc4408.txt

[b-contr-spam] "*Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*" (Code des Etats-Unis). Cet Acte est documenté dans les lois suivantes: 15 U.S.C. §§ 7701-7713; 18 U.S.C. § 1037; 28 U.S.C. § 994; 47 U.S.C. § 227. www.gpsaccess.gov/uscode/index.html

[b-ITU-T cyb] Rapports de la conférence du Groupe de travail contre l'utilisation abusive des messageries: www.itu.int/ITU-D/cyb/cybersecurity/spam.html

Annexe B

Gestion d’identité

UNION INTERNATIONALE DES TELECOMMUNICATIONS

UIT-T

SECTEUR DE NORMALISATION DES TÉLÉCOMMUNICATIONS DE L'UIT

Série X

Supplément 7

(02/2009)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATIONS ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Supplément relatif à la présentation de la gestion d'identité dans le cadre de la cybersécurité

ATTENTION !

RECOMMANDATION PRÉPUBLIEE

La présente prépublication est une version non publiée d'une recommandation récemment approuvée. Elle est destinée à être remplacée par la version publiée après l'édition. Par conséquent, des différences pourront survenir entre cette pré-publication et la version publiée.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIETE INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous www.itu.int/ITU-T/ipr/.

Supplément 7 aux Recommandations de la série X – Série UIT-T X.1250

Supplément relatif à la présentation de la gestion d'identité dans le cadre de la cybersécurité

Résumé

La question de la sécurité de fonctionnement du réseau traditionnel téléphonique public commuté (RTPC) est traitée depuis de nombreuses décennies. Cela n'est toutefois pas le cas des réseaux publics IP répartis qui comptent de nombreux fournisseurs de services, comme l'Internet ou les réseaux de nouvelle génération (NGN). Ces réseaux utilisent une plate-forme de transport commune pour le trafic de contrôle et le trafic utilisateur qui, en plus de l'anonymat possible de ce type de trafic et de la possibilité de générer un trafic unidirectionnel, expose ces réseaux à des utilisations abusives. Tous les services électroniques (tels que le commerce en ligne, le commerce électronique, la cybersanté, l'administration publique en ligne) peuvent subir des attaques informatiques. Ce problème peut être partiellement réglé si l'on améliore le niveau de confiance en termes d'identité des utilisateurs, des dispositifs réseau et des fournisseurs de services, qui pourront alors être authentifiés, recevoir un accès approprié et être contrôlés. Dans la mesure où la gestion d'identité fournit un niveau d'assurance et de confiance supérieurs en termes d'identité de l'utilisateur, du fournisseur de services et des dispositifs réseau, elle renforce la sécurité en limitant l'exposition aux risques de sécurité. Cet aspect de la cybersécurité doit être pris en compte, d'une part, par les fournisseurs de services au niveau des entreprises et, d'autre part, par les pouvoirs publics au niveau national dans le cadre de leur plan national sur la cybersécurité.

Introduction

La gestion d'identité (IdM) est un mode de gestion et de contrôle des informations utilisées dans le processus de communication pour représenter les entités (fournisseurs de services, organisations d'utilisateurs, individus, dispositifs réseau, applications et services de logiciel). Une seule et même entité peut compter des identités numériques multiples pour accéder à divers services ayant des exigences de sécurité différentes et celles-ci peuvent exister dans des emplacements multiples.

L'IdM est une composante essentielle de la cybersécurité en ce sens qu'elle permet d'établir et de maintenir des communications de confiance entre les entités. Elle permet d'authentifier une identité. Elle ouvre aussi droit à une série de privilèges d'accès (au lieu d'un accès tout ou rien) et permet de modifier facilement le niveau d'accès lorsque le rôle d'une entité change. L'IdM permet aussi à une organisation de veiller à ce que ses politiques de sécurité soient correctement appliquées moyennant le contrôle de l'activité d'accès de l'entité. Elle peut assurer l'accès à des entités tant à l'intérieur qu'à l'extérieur d'une organisation. En bref, une bonne solution IdM offre des moyens fiables d'authentifier les identités, de fournir et de gérer des identités d'entité et, enfin, de contrôler l'accès d'une entité.

L'IdM est un élément essentiel pour gérer la sécurité et permettre l'accès itinérant sur demande à des réseaux et à des cyberservices. Parallèlement à d'autres mécanismes défensifs (par exemple, pare-feu, systèmes de détection d'intrusion et protection contre les virus), l'IdM joue un rôle important dans la protection des réseaux et services d'information et de communication contre les délits informatiques tels que l'escroquerie et l'usurpation d'identité. Ainsi, les utilisateurs auront davantage confiance dans la sécurité et la fiabilité des transactions électroniques, ce qui facilite l'utilisation des réseaux IP pour les cyberservices.

La question fondamentale de la confidentialité doit être prise en compte lors de la mise en œuvre d'un système IdM. Cela implique l'élaboration de méthodes visant à garantir la précision des informations d'identité et à empêcher l'utilisation de ces informations à des fins autres que celles pour lesquelles elles ont été recueillies.

1 Champ d'application

La gestion d'identité s'est imposée comme un élément stratégique dans le renforcement de la sécurité en améliorant le niveau d'assurance par l'intermédiaire de la vérification de la validité des informations d'identité. Ce supplément offre une présentation générale de ce nouveau service.

L'utilisation du terme "identité" dans ce supplément relatif à la gestion d'identité ne lui confère pas une valeur absolue, et ne constitue pas en particulier une validation positive.

2 Références

Aucune.

3 Définitions

Les définitions sont disponibles dans d'autres recommandations de la série X.1250.

4 Abréviations et acronymes

IdM – Gestion d'identité

IP – Protocole Internet

RTPC – Réseau téléphonique public commuté

5 Conventions

Aucune.

6 Sécurité: importance pour l'infrastructure mondiale du réseau et coordination multinationale

La sécurité de l'infrastructure mondiale du réseau dépendra de la mise en œuvre et de l'utilisation appropriées des capacités et des pratiques d'IdM dans les différents réseaux nationaux, régionaux et internationaux. Il est important et nécessaire d'avoir de bonnes pratiques et une mise en œuvre appropriée afin de garantir les informations d'identité et l'intégrité et la disponibilité de l'infrastructure mondiale du réseau.

On peut utiliser des moyens IdM pour offrir des services nationaux et internationaux de télécommunication en situation d'urgence en identifiant les utilisateurs autorisés à fournir des services spéciaux.

En outre, ces moyens peuvent servir pour éviter, détecter et assurer la coordination des mesures à prendre pour faire face aux incidents de cybersécurité aux niveaux national et international. Dans certains cas, l'IdM peut aider les autorités et les entités à coordonner leurs efforts pour retracer et localiser la source de ces incidents.

7 La gestion d'identité comme catalyseur de communication de confiance entre deux entités

L'une des fonctions importantes de l'IdM est d'assurer l'authentification des utilisateurs, réseaux ou services. Dans un processus d'authentification impliquant deux entités, une entité affirme son identité à l'autre entité. Selon les exigences de la deuxième entité, il faut peut-être que ces affirmations soient validées pour que celle-ci ait suffisamment confiance en la première pour lui accorder des privilèges. Ce processus peut être requis dans les deux sens.

Plusieurs niveaux d'authentification sont disponibles (minimal ou nul, faible (par exemple, nom d'utilisateur et mot de passe), élevé (par exemple, l'infrastructure de clé publique (UIT-T X.509)). L'évaluation des risques permet d'identifier le niveau d'authentification approprié. Des niveaux d'authentification supérieurs peuvent être requis pour une entité spécifique, par exemple, si elle contrôle des ressources stratégiques.

8 Protection, maintenance, révocation et contrôle des données d'identité

L'IdM a d'autres fonctions importantes comme de protéger, préserver et contrôler les données d'identité de confiance, notamment la possibilité d'identifier le statut actuel d'une identité.

Les lois ou réglementations peuvent imposer une protection des informations personnellement identifiables et interdire l'utilisation des informations d'identité à des fins autres que celles pour lesquelles elles ont été recueillies. La garantie du maintien de la validité des données d'identité est un autre aspect important. Pour garantir la viabilité des services qui les utilisent, les données d'identité doivent être gérées de manière appropriée afin de préserver leur précision, leur ponctualité et leur cohérence.

La gestion des attributs des données d'identité doit inclure, si approprié, l'option de vérification des données d'identité afin de vérifier leur statut en termes de révocation.

Dans la majorité des cas, les entités souhaiteront contrôler l'utilisation de leurs données personnelles et de leurs informations privées.

9 "Découverte" de sources authentifiées de données d'identité

L'IdM recouvre également le concept de "découverte" des données d'identité authentifiées. Dans un environnement très réparti où coexistent de nombreux fournisseurs (comme l'Internet et les réseaux de nouvelle génération), les données d'identité nécessaires pour assurer l'authentification de l'identité et les assertions connexes peuvent être situées à différents emplacements sur le réseau. Les entités peuvent avoir des identités numériques multiples avec des sources d'informations d'identité différentes dans des emplacements divers. Lorsqu'une entité parmi les deux entités impliquées dans le processus d'authentification se déplace, l'autre entité devra envisager et établir une relation de confiance avec une source d'informations d'identité appropriée afin de compléter le processus d'authentification de l'entité itinérante. Le concept de découverte des sources d'informations authentifiées est un processus analogue à celui qui s'applique aujourd'hui à la téléphonie mobile cellulaire.

10 Services d'administration publique en ligne

Les avantages de la mise en œuvre de l'IdM pour une entité sont les suivants: réduction des risques, renforcement de la confiance, amélioration des fonctionnalités et réduction potentielle des coûts. Ces motifs de mise en œuvre d'un IdM s'appliquent également lorsque l'entité est une administration. Dans les services d'administration publique en ligne, les principaux objectifs sont également de diminuer les coûts et de fournir des services plus efficaces aux citoyens et aux partenaires commerciaux de l'administration.

Les pouvoirs publics, tout comme les autres entités, sont confrontés au problème qui consiste à utiliser efficacement les identités dans un monde interconnecté. Pour faire des services d'administration publique en ligne une réalité, les pouvoirs publics doivent réaliser des analyses de risque sur les cyberservices qu'ils ont l'intention de proposer et mettre en œuvre des mesures de protection appropriées. Compte tenu de la nature sensible de bon nombre de ces services d'administration publique en ligne (par exemple, la cybersanté), une administration peut être amenée à appliquer une méthode d'authentification rigoureuse.

11 Considérations relatives à la réglementation associée à l'IdM

Les administrations nationales et les groupes régionaux doivent prendre en considération un certain nombre de questions réglementaires potentielles associées à la mise en œuvre de l'IdM, comme la protection de la confidentialité et des données, la préparation aux situations d'urgence et à la sécurité nationale et les dispositions obligatoires entre les opérateurs. Les pouvoirs publics doivent non seulement utiliser des techniques de gestion d'identité mais également les imposer aux autres entités pour se conformer à un large éventail de règlements nationaux et d'objectifs de sécurité.

Bibliographie

Différents forums travaillent sur les questions concernant l'IdM, à savoir:
3GPP SA3: www.3gpp.org/SA3-Security?page=type_urls

ARK (Schéma de nommage de la *California Digital Library*): www.cdlib.org/inside/diglib/ark/

Carte européenne du citoyen: www.europa.eu.int/idabc/servlets/Doc?id=19132

ETSI TISPAN WG7: www.etsi.org/tispan/

Feuille de route de l'UE sur l'identité électronique (eID):
www.ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

FIDIS (UE – L'avenir de l'identité dans la société de l'information): www.fidis.net/

FIRST (Organisme de coordination des CERT): www.first.org/

Groupe d'étude sur l'ingénierie Internet: sec.ietf.org/

Handle: www.handle.net/

Higgins: www.eclipse.org/higgins/index.php

IDSP (*Identity Theft Prevention and Identity Management Standards Panel* (IDSP) de l'*American National Standards Institute*):
www.ansi.org/standards_activities/standards_boards_panels/idsp/overview.aspx?menuid=3

IGF (structure de gouvernance de l'identité d'Oracle):
www.oracle.com/technology/tech/standards/idm/igf/index.html

ITRC (*Identity Theft Resource Center*): www.idtheftcenter.org/

Liberty Alliance Project: www.projectliberty.org/

Light-Weight Identity: lid.netmesh.org/wiki/Main_Page

MODINIS-IDM Consortium: www.egov-goodpractice.org et
www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium

OASIS (Organisation pour la promotion des standards d'information structurée):

www.oasis-open.org/home/index.php

OCDE (Organisation pour la coopération et le développement économiques) – Atelier sur la gestion des identités numériques, Trondheim (Norvège), 8-9 mai 2007: www.oecd.org/sti/security-privacy/idm

OMA (*Open Mobile Alliance*): www.openmobilealliance.org

The Open Group: www.opengroup.org

OSIS (*Open Source Identity System*): osis.idcommons.net/wiki/Main_Page

PAMPAS (UE – *Pioneering Advanced Mobile Privacy and Security*): www.pampas.eu.org

PERMIS (UE – *Information Society Initiative in Standardization (ISIS), PrivilEge and Role*)

Prime (*EU Privacy and Identity Management for Europe*): www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium

Projet "Guide" (*Government User Identity for Europe*) de l'UE: www.ist-world.org/ProjectDetails.aspx?ProjectId=4ddb2e61c84343f0acd370607e5a8499&SourceDatabaseId=7cff9226e582440894200b751bab883f

Systèmes nationaux de cartes d'identité: www.homeoffice.gov.uk/passports-and-immigration/id-cards.en.wikipedia.org/wiki/Identity_document

UIT-T – Commission d'études 17 (sécurité), Groupe spécialisée sur la gestion des identités: www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

UIT-T – Question 10 de la Commission d'études 17 (sécurité):
www.itu.int/ITU-T/studygroups/com17/index.asp

UIT-T – Question 13 de la Commission d'études 13 (réseaux futurs):
www.itu.int/ITU-T/studygroups/com13/index.asp

W3C (*World Wide Web Consortium*): www.w3.org/

Yadis: yadis.org/wiki/Main_Page

Annexe C

Liens et références

Cette liste de documents de référence sera régulièrement mise à jour, compte tenu des résultats du Programme mondial cybersécurité de l'UIT, des résultats du projet de mise en œuvre de la Résolution 45 (CMDT-06), des travaux effectués par la Commission d'études 17 de l'UIT-T (Commission d'études directrice pour la sécurité à l'UIT-T), des Résolutions de l'AMNT ainsi que du suivi de la grande orientation C5 du SMSI sur la cybersécurité et des résultats des travaux concernant des Résolutions appropriées de la PP-06 (Résolutions 130, 131 et 149, par exemple).

Partie I: Elaborer et obtenir un accord concernant une stratégie nationale de la cybersécurité

I.C.1 Accroître la sensibilisation (I.B.1, I.B.2)

International

- Résolution 55/63 de l'Assemblée générale des Nations Unies: "Lutte contre l'exploitation des technologies de l'information à des fins criminelles ": www.un.org/Depts/dhl/resguide/r55.htm
- Résolution 56/121 de l'Assemblée générale des Nations Unies: "Lutte contre l'exploitation des technologies de l'information à des fins criminelles": www.un.org/Depts/dhl/resguide/r56.htm
- Résolution 57/239 de l'Assemblée générale des Nations Unies: "Création d'une culture mondiale de la cybersécurité ": www.un.org/Depts/dhl/resguide/r57.htm
- Résolution 58/199 de l'Assemblée générale des Nations Unies: "Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information ": un.org/Depts/dhl/resguide/r58.htm
- Sommet mondial des Nations Unies sur la société de l'information: Déclaration de principes et Plan d'action de Genève, engagement de Tunis et Agenda de Tunis pour la société de l'information: www.itu.int/WSIS/index.html
- Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: Vers une culture de la sécurité (2005): www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html
- Manuel international sur la protection des infrastructures essentielles de l'information, 2006 (Volume 1): www.isn.ethz.ch/pubs/ph/details.cfm?id=250
- Ressources de l'UIT sur la cybersécurité: www.itu.int/cybersecurity/
- Programme mondial cybersécurité de l'UIT: www.itu.int/cybersecurity/gca/
- Passerelle de cybersécurité de l'UIT: www.itu.int/cybersecurity/gateway/
- Page web consacrée à la cybersécurité, Bureau de développement des télécommunications de l'UIT: www.itu.int/ITU-D/cyb/
- Initiative Protection de l'enfance en ligne de l'UIT et lignes directrices connexes: www.itu.int/cop/

I.C.2 Stratégies nationales, régionales et internationales (I.B.2, I.B.3, I.B. 4, I.B.5, I.B.7)

International

- Kit de l'UIT pour l'auto-évaluation de l'état de préparation national dans le domaine de la cybersécurité/CIIP: www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

- UIT et ETH Zurich – Cadre générique national pour la protection des infrastructures essentielles de l'information CIIP: www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf
- Secteur du développement des télécommunications de l'UIT, Commission d'études 1, Question 22/1: Sécurisation des réseaux de l'information et de la communication: Bonnes pratiques pour créer une culture de la cybersécurité: www.itu.int/ITU-D/study_groups/SGP_2006-2010/documents/DEFQUEST-SG1/DEFQUEST-Q22-1-E.pdf
- Programme mondial cybersécurité de l'UIT: www.itu.int/cybersecurity/gca/
- Guide UIT de la cybersécurité pour les pays en développement, Rév. 2009: www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf
- UIT: Résolution 45 de la CMDT (Doha, 2006): Mécanismes propres à améliorer la coopération en matière de cybersécurité, y compris la lutte contre le spam: itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-f.pdf
- Secteur de la normalisation des télécommunications de l'UIT, Commission d'études 17, Question 4, Manuel sur la sécurité – Catalogue des Recommandations approuvées par l'UIT-T concernant la sécurité des télécommunications: www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000090003MSWE.doc
- Secteur de la normalisation des télécommunications de l'UIT, Commission d'études 17, Question 4 – Sécurité dans les télécommunications et les technologies de l'information: www.itu.int/pub/T-HDB-SEC.03-2006/en/
- UIT – Etude du BDT sur les aspects financiers de la sécurité des réseaux: Logiciels malveillants et spams: www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf
- Lignes directrices de l'OCDE régissant la sécurité des systèmes et des réseaux de l'information: Vers une culture de la sécurité: www.oecd.org/document/42/0,3343,en_21571361_36139259_15582250_1_1_1_1,00.html
- Plan d'action de l'OCDE pour la mise en œuvre concertée des politiques nationales de sécurité en ligne: www.oecd.org/dataoecd/23/11/31670189.pdf
- Rapport de la Banque mondiale "Cybersécurité: un nouveau modèle de protection du réseau ": www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2006/12/12/000020953_20061212113151/Rendered/PDF/381170CyberSec1uly0250200601PUBLIC1.pdf
- *Information Technology Association of America* (ITAA), White Paper on Information Security: www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf

Régional

- APEC Telecom and Information Working Group – APEC Cybersecurity Strategy (2002): unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf
- Livre bleu de la CITEL: Politiques de télécommunication pour les Amériques (2005) sections 8.4-8.5: www.citel.oas.org/publications/azul-fin-r1c1_i.pdf
- Résolution du Conseil de l'Union européenne: Stratégie pour une société de l'information sûre – Dialogue, partenariat et responsabilisation (2007): eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf
- Déclaration de Doha sur la cybersécurité (2008): www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-regional-cybersecurity-forum-output-20-feb-08.pdf

- Communication de l'Union européenne "Une stratégie pour une société de l'information sûre" (2006): ec.europa.eu/information_society/doc/com2006251.pdf
- Programme de l'Union européenne pour un Internet plus sûr: europa.eu.int/information_society/activities/sip/index_en.htm
- Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) – Etude sur les aspects économiques de la sécurité et le marché intérieur (2008): www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm
- Organisation des Etats américains – Stratégie interaméricaine de lutte contre les menaces qui pèsent sur la cybersécurité (2004): www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

National

- *Australia's Critical Infrastructure Protection Modelling and Analysis Program* (CIPMA): www.csiro.au/partnerships/CIPMA.html
- *Crisis and Risk Network (CRN), International CIIP Handbook: An Inventory and Analysis of National Protection Policies*: www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250
- Plan national de l'Allemagne pour la protection des infrastructures de l'information: www.bmi.bund.de/cln_028/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure__Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.pdf
- Stratégie nationale du Japon sur la sécurité de l'information (traduction provisoire): www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf
- Stratégies nationales de mise en œuvre de 11 pays membres de l'OCDE: www.oecd.org/document/63/0,2340,en_21571361_36139259_36306559_1_1_1_1,00.html
- Stratégie numérique de la Nouvelle-Zélande: www.digitalstrategy.govt.nz
- Singapore's Infocomm Security Masterplan 2: www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20080417090044/MR17Apr08MP2.pdf
- Stratégie de Singapour pour la sécurisation du cyberespace: www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21
- Royaume-Uni – Centre for the Protection of National Infrastructure (CPNI): www.cpni.gov.uk/
- Etats-Unis – National Strategy to Secure Cyberspace: www.whitehouse.gov/

I.C.3 Evaluation et élaboration de programmes (I.B.5, I.B.7, I.B.8)

- Control Objectives for Information and Related Technology (COBIT) 4.1: www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981 (résumé analytique gratuit; inscription nécessaire pour télécharger la version complète).
- *Information Technology Infrastructure Library (ITIL) Security Management*: www.itil-itsm-world.com (redevance requise).
- Organisation internationale de normalisation/Commission électrotechnique internationale (ISO/CEI) – série 27000, Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information: www.iso27001security.com/index.html
- ISO/CEI 13335, Technologies de l'information – Techniques de sécurité – Gestion de la sécurité des technologies de l'information et des communications – Partie 1: Concepts et modèles pour la gestion de la sécurité des technologies de l'information et des communications: www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39066 (redevance requise).

- ISO/CEI 17799, 2005, Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la gestion de la sécurité de l'information: www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612 (redevance requise).
- ISO/CEI 21827, Ingénierie de sécurité systèmes – Modèle de maturité de capacité (SSE-CMM®): www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34731 (redevance requise)
- UIT – Etude du BDT sur les aspects financiers de la sécurité des réseaux: Logiciels malveillants et spams: www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf
- UIT – Résolution 50 de l'AMNT (Rév. Johannesburg, 2008) sur la cybersécurité: www.itu.int/dms_pub(itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf
- UIT- Résolution 52 de l'AMNT (Rév. Johannesburg, 2008)" Lutter contre et combattre le spam": www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-F.pdf
- UIT – Résolution 58 de l'AMNT (Johannesburg, 2008) "Encourager la création d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement": www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2008-PDF-F.pdf
- Publication spéciale 800-12 du NIST – An Introduction to Computer Security: The NIST Handbook (février 1996): www.csrc.nist.gov/publications/nistpubs/800-12/
- Publication spéciale 800-30 du NIST – Risk Management Guide for Information Technology Systems (Juillet 2002): csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Projet de publication spéciale 800-53 du NIST – Recommended Security Controls for Federal Information Systems (décembre 2007): csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
- Publication spéciale 800-53A du NIST – Guide for Assessing the Security Controls in Federal Information Systems (décembre 2007): csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-A
- Publication spéciale 800-50 du NIST – Building an Information Technology Security Awareness and Training Program (octobre 2003): csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
- Publication spéciale 800-30 du NIST – Risk Management Guide for Information Technology Systems, (juillet 2002): csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVESM): www.cert.org/octave/

I.C.4 Points de contact d'assistance internationale (I.B.6)

- Anti-Phishing Working Group (APWG): www.antiphishing.org
- Forum of Incident Response Security Teams (FIRST): www.first.org
- Institut des ingénieurs en électricité et en électronique: www.ieee.org
- Groupe d'étude sur l'ingénierie Internet: www.ietf.org
- Messaging Anti-Abuse Working Group: www.maawg.org
- World Information Technology Services Alliance: www.witsa.org
- World Wide web Consortium: www.w3c.org

PARTIE II – Etablir une collaboration au niveau national entre les pouvoirs publics et l'industrie

II.C.1 Structures de collaboration pouvoirs publics/industrie

International

- *Cyber Security Industry Alliance*: www.csialliance.org/about_csia/index.html

- Boîte à outils antispam de l'OCDE – Partenariats de coopération contre le spam: www.oecd-antispam.org/article.php3?id_article=243
- StopSpamAlliance.org: stopspamalliance.org/

Régional

- Moyen-Orient: Report on 14th GCC eGovernment and eServices Forum: www.zawya.com/Story.cfm/sidZAWYA20080529073202/SecMain/pagHomepage/chnAll%20Regional%20News/obj2A17E941-F5E0-11D4-867D00D0B74A0D7C/

National

- Australie – Business-Government Partnership: The Trusted Information Sharing Network for Critical Infrastructure Protection: www.tisn.gov.au/www/tisn/tisn.nsf/Page/CIPPrograms_CriticalInfrastructureProtectionModellingandAnalysis(CIPMA)
- Etats-Unis - Centres d'analyse et d'échange d'informations (ISAC) et Conseils de coordination:
  - ISAC des services financiers www.fsisac.com/
  - ISAC du secteur de l'électricité www.esisac.com/
  - ISAC des technologies de l'information www.it-isac.org
  - ISAC des télécommunications www.ncs.gov/ncc/
  - Network Reliability and Interoperability Council (Conseil chargé de la fiabilité et de l'interopérabilité du réseau) (NRIC): www.nric.org/
  - National Security and Telecommunications Advisory Committee (Comité consultatif chargé de la sécurité nationale et des télécommunications) (NSTAC):www.ncs.gov/nstac/nstac.html
- Etats-Unis – Coopération industrie-pouvoirs publics en matière de normalisation: American National Standards Institute-Homeland Security Standards Panel: www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3
- Etats-Unis – Livre blanc de l'Information Technology Association of America sur la sécurité de l'information: www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf
- Etats-Unis – IT Sector Coordinating Council (SCC): www.it-scc.org
- Etats-Unis – Partenariat national sur la cybersécurité: www.cyberpartnership.org/
- Etats-Unis – Rapport du Groupe de travail du National Information Assurance Council (NIAC) sur le modèle de partenariat sectoriel: itaa.org/eweb/upload/NIAC_SectorPartModelWorkingGrp_July05.pdf
- Etats-Unis - Plan de protection de l'infrastructure nationale: www.dhs.gov/xprevprot/programs/editorial_0827.shtm
- Etats-Unis - Plans spécifiques du secteur: www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm
- Etats-Unis – Plan spécifique du secteur informatique: www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf
- Etats-Unis - National Telecommunications and Information Administration: www.ntia.doc.gov/

II.C.2 Partage d'informations concernant la cybersécurité

International

- Messaging Anti-Abuse Working Group: www.maawg.org

National

- Etats-Unis – NIST – Computer Security and Research Center: csrc.nist.gov/
- Etats-Unis – Alertes du CERT: www.us-cert.gov/cas/

II.C.3 Amélioration de la sensibilisation et ouverture: outils pour utilisations professionnelle et privée

International

- Elaboration d'un programme de sensibilisation sur la sécurité: www.gideonrasmussen.com/article-01.html
- Centre de ressources sur la sécurité de l'Internet et de publications sur la sécurité des entreprises: www.cisecurity.org/resources.html
- Stratégies des entreprises pour la sensibilisation sur la sécurité: articles.techrepublic.com.com/5100-10878_11-5193710.html
- Guide sur la cybersécurité à l'intention des petites entreprises: www.uschamber.com/publications/reports/0409_hs_cybersecurity.htm
- EDUCAUSE - Ressources de sensibilisation sur la sécurité à l'intention des pouvoirs publics et des entreprises: www.educause.edu/Security%20Task%20Force/CybersecurityAwarenessResource/BrowseSecurityAwarenessResourc/8770?time=1215527945
- ENISA - Initiatives de sensibilisation sur la sécurité de l'information (existe en plusieurs langues): www.enisa.europa.eu/Pages/05_01.htm
- Interpol - Méthodes de prévention de la criminalité et de sécurité informatique (prévention des délits dans les entreprises): www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp
- Interpol IT Crime Company Checklist: www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp
- NoticeBored Security Awareness Posters: www.noticebored.com/html/posters.html
- Boîte à outils antispam de l'OCDE - Education et sensibilisation: www.oecd-antispam.org/article.php3?id_article=242
- SANS Security Policy Resources: www.sans.org/resources/policies/
- Security Awareness Toolbox – The Information Warfare Site: www.iwar.org.uk/comsec/resources/sa-tools/
- Etats-Unis - Partenariat national sur la cybersécurité - Sensibilisation des petites entreprises et centre de ressources pour les petites entreprises: www.cyberpartnership.org/init-aware.html

National

- United States Federal Trade Commission: www.ftc.gov/infosecurity
- Publication 800-50 du NIST – Security Awareness and Training Program: csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

PARTIE III – Prévenir la cybercriminalité/fondements juridiques et mise en application

International

- Conseil de l'Europe: Convention sur la cybercriminalité du Conseil de l'Europe (2001): www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp
- G8 – Principes concernant la criminalité liée à la haute technologie: www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html
- Passerelle sécurité de l'UIT: Texte de base relatif à l'harmonisation des approches juridiques nationales, à la coordination juridique au niveau international et aux mesures d'application: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
- Kit pratique UIT/InfoDev sur la régulation des TIC: www.ictregulationtoolkit.org/
- Publication de l'UIT "Comprendre la cybercriminalité: guide pour les pays en développement": www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html

- Kit pratique de l'UIT pour la législation relative à la cybercriminalité: www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html
- Interpol Information Technology Crime Resources: www.interpol.com/Public/TechnologyCrime/
- Approches de l'OCDE en matière de régulation antispam: www.oecd-antispam.org/article.php3?id_article=1
- Boîte à outils antispam de l'OCDE: www.oecd-antispam.org/article.php3?id_article=265
- Résolution 55/63 de l'Assemblée générale des Nations Unies: "Lutte contre l'exploitation des technologies de l'information à des fins criminelles": www.un.org/Depts/dhl/resguide/r55.htm
- Résolution 56/121 de l'Assemblée générale des Nations Unies: "Lutte contre l'exploitation des technologies de l'information à des fins criminelles": www.un.org/Depts/dhl/resguide/r56.htm
- Ressources de l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice pour améliorer les connaissances et créer de nouveaux partenariats destinés à lutter contre la cybercriminalité: www.unicri.it/
- Lois-types de la CNUDCI sur le commerce électronique et les signatures électroniques: www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html
- Office des Nations Unies contre la drogue et le crime: www.unicri.it/

Régional

- APEC: documents, exposés et déclarations ministérielles concernant la criminalité: www.apectelwg.org/
- Déclaration du Caire – Conférence sur la cybercriminalité: www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_EN.pdf
- Loi-type du Commonwealth sur les délits informatiques et les délits connexes: www.thecommonwealth.org/Internal/38061/documents/
- Conseil de l'Europe: Convention sur la criminalité (2001): www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp
- Organisation des Etats américains: Portail de coopération interaméricain sur la cybercriminalité: www.oas.org/juridico/english/cyber.htm

National

- Centre de coordination CERT: Comment le FBI enquête sur la criminalité informatique: www.cert.org/tech_tips/FBI_investigates_crime.html
- Législation sur la cybercriminalité: Etude sur les législations relatives à la cybercriminalité dans le monde: www.cybercrimelaw.net/index.html
- Conseil de l'Europe: Etude des législations nationales en matière de cybercriminalité: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/Legprofiles.asp#TopOfPage
- Microsoft: "Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws ": www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf
- Législation antispam des Etats Membres de l'OCDE: www.oecd-antispam.org/countrylaws.php3
- Nations Unies – "Modèles de cyberlégislation dans les pays membres de la Commission économique et sociale pour l'Asie occidentale (ESAO)": www.escwa.un.org/information/publications/edit/upload/ictd-07-8-e.pdf
- Etats-Unis - Site web de la Section délits informatiques et propriété intellectuelle du Département de la justice: www.cybercrime.gov
- Etats-Unis - Département de la justice - Manuel sur les poursuites contre la criminalité informatique (Chapitre 1 – Loi contre l'abus et la fraude informatique): www.cybercrime.gov/ccmanual/

- Etats-Unis – Secret Service – Best Practices for Seizing Electronic Evidence: www.forwardedge2.com/pdf/bestPractices.pdf

Partie IV: Créer au niveau national des structures de gestion des incidents: surveillance, alerte, intervention et retour a la normale

IV.C.1 Plan national d'intervention et Centre CSIRT national

International

- Carnegie Mellon University: Centre de coordination CERT: www.cert.org/csirts/
- Centre de coordination CERT: Liste de mesures à prendre pour créer un CSIRT: www.cert.org/csirts/action_list.html
- Centre de coordination CERT: Guide de création d'un CSIRT: www.cert.org/csirts/Creating-A-CSIRT.html
- Centre de coordination CERT: Définir les processus de gestion des incidents pour les CSIRT: activité en cours: www.cert.org/archive/pdf/04tr015.pdf
- Centre de coordination CERT: Questions fréquemment posées sur les CSIRT: www.cert.org/csirts/csirt_faq.html
- Centre de coordination CERT: Manuel sur les CSIRT: www.cert.org/archive/pdf/csirt-handbook.pdf
- Centre de coordination CERT: Evaluation des capacités de gestion des incidents – Version 0.1: www.cert.org/archive/pdf/07tr008.pdf
- Centre de coordination CERT: Modèles d'organisation des CSIRT: www.cert.org/archive/pdf/03hb001.pdf
- Centre de coordination CERT: Services CSIRT: www.cert.org/csirts/services.html
- Centre de coordination CERT: Effectifs d'un centre CSIRT – Compétences de bases requises: www.cert.org/csirts/csirt-staffing.html
- Centre de coordination CERT: Les CSIRT: état des lieux: www.cert.org/archive/pdf/03tr001.pdf
- Centre de coordination CERT: Etapes de la création de CSIRT nationaux: www.cert.org/archive/pdf/NationalCSIRTs.pdf
- Environnement de formation virtuelle (VTE): www.vte.cert.org/
- ENISA: Guide de création d'un CSIRT pas à pas: www.enisa.europa.eu/pages/05_01.htm
- Collaboration UIT-IMPACT et ressources connexes: itu.int/ITU-D/cyb/cybersecurity/impact.html
- GOVCERT.nl: CSIRT in a Box – Information on Setting up a CSIRT: www.govcert.nl/render.html?it=69
- Royaume-Uni – CPNI: The Warning, Advice and Reporting Point (WARP) Toolbox: www.warp.gov.uk/

Régional

- CERT Asie-Pacifique: www.apcert.org/index.html
- Ressources européennes en réseaux CSIRT: www.ecsirt.net/
- Groupe des CERT des gouvernements européens (EGC): www.egc-group.org/

National

- Australie: AusCERT: www.auscert.org.au
- Autriche: CERT.at: www.cert.at
- Brésil: CERT.br: www.cert.br/
- Chili: CLCERT: www.clcert.cl/
- Chine: CNCERT/CC: www.cert.org.cn/
- Finlande: CERT-FI: www.cert.fi

- Hongrie: CERT-Hungary: www.cert-hungary.hu
- Inde: CERT-In: www.cert-in.org.in
- Italie: CERT-IT: www.security.dico.unimi.it/
- Japon: JPCERT/CC: www.jpcert.or.jp/
- Corée: KrCERT/CC: www.krcert.or.kr/
- Malaisie: MyCERT: www.cybersecurity.org.my
- Pays-Bas: www.csirt.dk/
- Pologne: CERT POLSKA: www.cert.pl/
- Slovénie: SI-CERT: www.arnes.si/en/si-cert/
- Singapour: SingCERT: www.singcert.org.sg/
- Suède: SITIC: www.sitic.se
- Suisse: MELANI: www.melani.admin.ch
- Thaïlande: ThaiCERT: www.thaicert.nectec.or.th/
- Tunisie: CERT-TCC: www.ansi.tn/en/about_cert-tcc.htm
- Qatar: www.qcert.org
- Emirats arabes unis: www.aecert.ae/
- Plan national d'intervention des Etats-Unis: www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml
- CERT des Etats-Unis: www.us-cert.gov/
- Autres sites web nationaux sur les CERT/CSIRT

IV.C.2 Coopération et partage d'informations

International

- Centre de coordination CERT: Security vulnerabilities and fixes: www.cert.org/nav/index_red.html
- Centre d'échange pour les outils de gestion des incidents (CHIHT): chiht.dfn-cert.de/
- Forum des équipes de sécurité et d'intervention en cas d'incidents (FIRST) – ressources: www.first.org/
- Ressources des fournisseurs de services Internet en matière de services d'appui pour la sécurité: www.donelan.com/ispsupport.html
- Passerelle sécurité de l'UIT: texte de base relatif aux dispositifs de veille, d'alerte et d'intervention en cas d'incident: www.itu.int/cybersecurity/gateway/watch_warning.html
- Système d'alerte ITsafe pour les petites entreprises et les particuliers: www.itsafe.gov.uk/
- Boîte à outils antispam de l'OCDE: http://www.oecd-antispam.org/article.php3?id_article=265

Régional

- Trans-European Research and Education Networking Association (TERENA): www.terena.org/

National

- Pays-Bas – Service national d'alerte des Pays-Bas: www.waarschuwingsdienst.nl/render.html?cid=106
- Royaume-Uni – CPNI: *The Warning, Advice and Reporting Point (WARP) Toolbox*: www.warp.gov.uk/
- Etats-Unis – IT-ISAC: https://www.it-isac.org/
- Etats-Unis – IT Sector Coordinating Council (ISCC): Information Technology: Critical *Infrastructure and Key Resources Sector-Specific Plan*: www.it-scc.org/documents/itscc/Information_Technology_SSP_2007.pdf
- Etats-Unis – *National Institute of Standards and Technology (NIST)*: csrc.nist.gov/

IV.C.3 Informations sur la vulnérabilité/les outils et techniques

- Build Security In (Intégrer la sécurité) – Recueil d'informations sur la certification et la sécurité des logiciels visant à favoriser la création de systèmes sécurisés: www.buildsecurityin.us-cert.gov/daisy/bsi/home.html
- Common Vulnerabilities and Exposures List (CVE) (Liste des vulnérabilités et des failles): www.cve.mitre.org/about/
- Open Vulnerability Assessment Language (OVAL): oval.mitre.org/
- Etats-Unis – For software National Vulnerability Database (NVD): nvd.nist.gov/nvd.cfm

Partie V: Promouvoir une culture nationale de la cybersécurité

V.C.1 Systèmes et réseaux des pouvoirs publics (V.B.1, V.B.2, V.B.7)

International

- Grande orientation C5 du Plan d'action du SMSI: www.itu.int/wsis/implementation/index.html
- Programme mondial UIT sur la cybersécurité: www.itu.int/osg/csd/cybersecurity/gca/
- UIT – Réunion thématique du SMSI visant à lutter contre le spam: www.itu.int/osg/spu/spam/meeting7-9-04/index.html
- Grande orientation C5 du SMSI – Première réunion – Rapport du Président: www.itu.int/osg/spu/cybersecurity/2006/chairmansreport.pdf
- Grande orientation C5 du SMSI – Deuxième réunion – Rapport du Président: www.itu.int/wsis/docs/geneva/official/poa.html
- Ordre du jour de la Deuxième réunion et liens vers les exposés: www.itu.int/osg/csd/cybersecurity/WSIS/meetingAgenda.html
- Grande orientation C5 du SMSI – Rapport de la Troisième réunion: www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf
- Ordre du jour de la Troisième réunion et liens vers les exposés: www.itu.int/osg/csd/cybersecurity/WSIS/agenda-3_new.html
- Microsoft: Computing Privacy, Internet Safety and Security Information for Policymakers Worldwide: www.microsoft.com/mscorp/twc/policymakers_us.mspx
- Portail de l'OCDE sur la culture de la sécurité et ressources connexes: ww.oecd.org/sti/cultureofsecurity
- OCDE, "Lignes directrices régissant la sécurité des systèmes et des réseaux d'information: Vers une culture de la sécurité" (2002): www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html
- OCDE: "Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel (1980)": www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html
- Rapport de l'OCDE "Promouvoir une culture de la sécurité pour les systèmes et réseaux de l'information dans les pays de l'OCDE" (2005): www.oecd.org/dataoecd/16/27/35884541.pdf
- Banque mondiale – Manuel sur la sécurité des technologies de l'information – Sécurité de l'information et politiques des pouvoirs publics: www.infodev-security.net/handbook/part4.pdf
- Résolution 57/239 de l'Assemblée générale des Nations Unies (Annexes A et B): www.un.org/Depts/dhl/resguide/r57.htm

Régional

- ENISA: "Initiatives de sensibilisation à la sécurité de l'information: pratiques actuelles et évaluation des résultats" (2007): www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf
- ENISA: "Guide à l'intention des utilisateurs: Comment sensibiliser davantage à la sécurité de l'information" (2006): www.enisa.europa.eu/doc/pdf/deliverables/enisa_a_users_guide_how_to_raise_IS_awareness.pdf
- Source d'information européenne sur la sécurité de l'Internet (InSafe): www.saferinternet.org/ww/en/pub/insafe/index.htm
- Organisation des Etats américains: Stratégie interaméricaine de lutte contre les menaces qui pèsent sur la cybersécurité: approche multidimensionnelle et pluridisciplinaire en vue de la création d'une culture de la cybersécurité (en particulier les Appendices) (2004): www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

National

- Brésil: ressources du site Antispam.br: antispam.br/
- Brésil: lignes directrices du Comité directeur brésilien sur l'Internet relatives à la sécurité de l'Internet (CGI.br): cartilha.cert.br/
- Initiatives de l'OCDE visant à promouvoir une culture de la sécurité (par pays): www.oecd.org/document/63/0,3343,en_21571361_36139259_36306559_1_1_1_1,00.html
- Etats-Unis – Site du CERT: www.us-cert.gov/
- Etats-Unis – *DHS National Critical Infrastructure Protection R&D Plan*: www.dhs.gov/xres/programs/gc_1159207732327.shtm
- Etats-Unis – *Federal Agency Security Practices*: csrc.nist.gov/fasp/
- Etats-Unis – *Federal Acquisition Regulation (FAR)*, parts 1, 2, 7, 11 and 39: www.acqnet.gov/FAR/
- Etats-Unis – *Federal Plan for Cyber Security and Information Assurance R&D*: www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf
- Etats-Unis – *Information Security and Privacy Advisory Board*: csrc.nist.gov/ispab/
- Etats-Unis – *Homeland Security Presidential Directive/HSPD-7*, "Critical Infrastructure Identification, Prioritization and Protection": www.whitehouse.gov/news/releases/2003/12/20031217-5.html
- Etats-Unis – *Multi-State Information Sharing and Analysis Center*: www.msisac.org/
- Etats-Unis – *National Strategy to Secure Cyberspace*: www.whitehouse.gov/pcipb/
- Etats-Unis – *President's Information Technology Advisory Committee Report on Cybersecurity Research Priorities*: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

V.C.2 Organisations du monde des affaires et du secteur privé (V.B.3., V.B.5., V.B.7.)

- Mouvement brésilien pour un Internet sûr: www.internetsegura.org/
- Centre de sécurité de Cisco (Section Bonnes pratiques): tools.cisco.com/security/center/home.x
- Microsoft Trustworthy Computing: www.microsoft.com/mscorp/twc/default.mspx
- NIATEC – Matériels didactiques: niatec.info/index.aspx?page=105
- Banque mondiale – Manuel sur la sécurité des technologies de l'information – La sécurité pour les organisations: www.infodev-security.net/handbook/part3.pdf
- Etats-Unis – Affiches et plaquettes d'information du CERT pour le lieu de travail: www.uscert.gov/reading_room/distributable.html
- Etats-Unis – Exercices de "cybertempête" du Department of Homeland Security (DHS): www.dhs.gov/xnews/releases/pr_1158340980371.shtm

V.C.3 Les particuliers et la société civile (V.B.4., V.B.6, V.B.7.)

- Brésil: SaferNet Brasil: www.safernet.org.br/site/
- *Be Safe Online* (SUSI – *Safer Use of Services on the Internet*): www.besafeonline.org/
- *CASES contact security tips*: casescontact.org/tips_list.php
- *Childnet International* – ressources pour les enfants: www.childnet-int.org
- *Cyber Peace Initiative*: www.cyberpeaceinitiative.org/
- CyberTipline: Apprendre aux adolescents comment naviguer sans danger: tcs.cybertipline.com/
- Internet Safety Zone – ressources pour les enfants et leurs parents: www.internetsafetyzone.co.uk/
- Interpol: Liste de conseils à suivre pour prévenir la cybercriminalité: www.interpol.int/Public/TechnologyCrime/CrimePrev/privateChecklist.asp
- Initiative "Protection de l'enfance en ligne" de l'UIT et lignes directrices connexes: www.itu.int/cop/
- GetNetWise – outils pour la famille: kids.getnetwise.org/tools/
- OnGuard Online – conseils pour se protéger des fraudes: onguardonline.gov/index.html
- MakeItSecure – informations sur les dangers commun d'Internet: www.makeitsecure.org/en/index.html
- Malaisie – initiatives en matière de cybersécurité: www.esecurity.org.my/
- NetSmartz: ressources pour les parents et les tuteurs: www.netsmartz.org/netparents.htm
- Nouvelle-Zélande – Netsafe: www.netsafe.org.nz
- SafeLine – assistance téléphonique pour dénoncer du contenu illégal: www.safeline.gr/
- Security Cartoon: www.securitycartoon.com/
- Stay Safe Online: www.staysafeonline.info/
- WiredSafety.org: www.wiredsafety.org/
- Banque mondiale – Manuel sur la sécurité des technologies de l'information: Sécurité des particuliers: www.infodev-security.net/handbook/part2.pdf
- Royaume-Uni – Ressources du centre contre l'exploitation des enfants et pour la protection des enfants en ligne (Child Exploitation and Online Protection Centre): www.ceop.gov.uk/
- United Kingdom's Get Safe Online: www.getsafeonline.org/
- Centre CERT des Etats-Unis pour les utilisateurs non professionnels

Autres initiatives de sensibilisation au niveau international, régional ou national pour les utilisateurs finals.

Imprimé en Suisse
Genève, 2010