Nations Unies A/66/152

Assemblée générale

Distr. générale
15 juillet 2011
Français
Original : anglais/russe

Soixante-sixième session
Point 93 de l'ordre du jour provisoire*
Les progrès de l'informatique et de la télématique et la question de la sécurité internationale

Les progrès de l'informatique et de la télématique et la question de la sécurité internationale

Rapport du Secrétaire général

Table des matières

* A/66/150.

11-41692X (F)

I. Introduction

1. Au paragraphe 3 de sa résolution 65/41, l'Assemblée générale invite tous les États Membres à continuer de communiquer au Secrétaire général, en tenant compte des constatations et recommandations figurant dans le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale[1], leurs vues et observations sur les questions suivantes :

a) L'ensemble des problèmes qui se posent en matière de sécurité de l'information;

b) Les efforts engagés au niveau national pour renforcer la sécurité de l'information et les activités de coopération internationale menées dans ce domaine;

c) La teneur des principes visés au paragraphe 2 de la résolution;

d) Les mesures que la communauté internationale pourrait prendre pour renforcer la sécurité de l'information à l'échelon mondial.

2. Comme suite à cette demande, une note verbale a été adressée aux États Membres le 16 mars 2011 pour les inviter à communiquer des informations à ce sujet. Les réponses reçues sont reproduites dans la section II ci-dessous. Les autres réponses reçues seront publiées sous forme d'additifs au présent rapport.

II. Réponses reçues des Gouvernements

Allemagne

[Original : anglais]
[6 juin 2011]

La situation en matière de sécurité dans le cyberespace a fondamentalement changé ces dernières années. D'un côté, nous assistons à un processus d'innovation axé sur la technologie sur le lieu de travail puisque de plus en plus de processus opérationnels sont gérés électroniquement et interconnectés et sont directement ou indirectement reliés à l'Internet. Les systèmes de technologies de l'information deviennent toujours plus complexes et les cycles d'innovation raccourcissent sans cesse. D'un autre côté, les protagonistes du crime organisé et autres acteurs non étatiques s'attaquent aux réseaux informatiques, aux bases de données et aux sites Web. Dans certains cas, ces attaques ont des répercussions qui n'ont pas encore été évaluées de manière réaliste.

Pour cette raison, en février 2011, le Gouvernement fédéral a adopté une nouvelle stratégie en matière de cybersécurité, principalement axée sur la protection des infrastructures critiques. Toutes les autorités gouvernementales confrontées aux problèmes de la cybersécurité doivent coopérer étroitement et directement l'une avec l'autre et avec le secteur privé au sein d'un nouveau centre national de cyberdéfense afin de détecter et analyser rapidement les principaux incidents dans le domaine des technologies de l'information et de recommander des mesures de protection. En ce qui concerne les politiques à mener, le nouveau Conseil national

[1] A/65/201.

de la cybersécurité et les secrétaires d'État qui le composent se penchent sur les questions fondamentales de la cybersécurité et sur la position de l'Allemagne à leur égard.

Il s'agit à cet égard de coordonner les politiques étrangères en matière de cybersécurité, en ce compris les aspects des politiques de défense et de sécurité et des politiques étrangères et économiques. Au vu des interconnexions internationales dans le cyberespace, une action coordonnée au niveau international s'avère essentielle. Au sein de l'Union européenne et dans les organisations internationales, l'Allemagne recommande donc vivement une cybersécurité accrue.

Dans le cadre de sa stratégie en matière de cybersécurité et compte tenu de l'interconnexion mondiale des technologies de l'information, l'Allemagne préconise l'élaboration de normes générales, non contentieuses et politiquement contraignantes relatives au comportement étatique dans le cyberespace. Elles doivent s'appliquer à une grande partie de la communauté internationale et comprendre des mesures visant à renforcer la confiance et à augmenter la sécurité.

Mesures de confiance et de sécurité dans le cyberespace

Le cyberespace est un bien public et un espace public. En tant que tel, nous devons considérer la sécurité du cyberespace en termes de résistance des infrastructures ainsi que d'intégrité et de sécurité des données en cas de panne des systèmes. Étant donné qu'il s'agit d'un espace public, les États doivent promouvoir la sécurité dans le cyberespace, en particulier à l'égard d'activités criminelles et malveillantes, en protégeant ceux qui choisissent d'utiliser des outils de validité pour contrer l'usurpation d'identité et en assurant l'intégrité et la confidentialité des données et des réseaux.

Le cyberespace est par nature mondial. La garantie de la cybersécurité, l'application des droits et la protection des infrastructures essentielles de l'information demandent un effort considérable de la part de l'État, à la fois au niveau national et en collaboration avec des partenaires internationaux.

Dans ce contexte, l'Allemagne est disposée à travailler sur une série de normes comportementales régissant le comportement mutuel des États dans le cyberespace, y compris, en particulier, sur des mesures particulières de renforcement de la confiance, de la transparence et de la sécurité, qui seront signées par le plus grand nombre possible de pays.

L'Allemagne a exposé récemment les éléments potentiels d'un tel code de conduite relatif aux normes internationales, lors de la conférence de l'organisation pour la sécurité et la coopération en Europe sur la cybersécurité, qui s'est tenue les 9 et 10 mai 2011, comme suit :

a) Confirmer les principes généraux de la disponibilité, la confidentialité, la concurrence, l'intégrité et l'authenticité des données et des réseaux, la vie privée et la protection des droits de propriété intellectuelle;

b) Respecter l'obligation de protéger les infrastructures essentielles;

c) Promouvoir la coopération visant à renforcer la confiance, les mesures de réduction des risques, la transparence et la stabilité par les moyens suivants :

- Échange de stratégies nationales, de meilleures pratiques et de perceptions nationales en invoquant la réglementation internationale du cyberespace;
- Échange de vues nationales eu égard aux normes juridiques internationales liées à l'utilisation du cyberespace;
- Mise en place et notification de points de contact;
- Mise en place de mécanismes d'alerte précoce et renforcement de la coopération, notamment entre les équipes d'intervention informatique d'urgence;
- Amélioration des liens de communication de crise afin de couvrir les cyberincidents, aide à la formulation de recommandations techniques visant à favoriser la solidité et la sécurité des cyberinfrastructures mondiales;
- Engagement responsable dans la lutte contre le terrorisme, y compris par l'échange de pratiques et une coopération renforcée en matière de mesures à prendre à l'encontre d'acteurs non étatiques;
- Aide au renforcement des capacités en matière de cybersécurité dans les pays en développement et élaboration de mesures volontaires d'aide en matière de cybersécurité dans le cadre de grandes manifestations (par exemple, les jeux olympiques).

En outre, nous estimons nécessaire de lancer un débat sur une coopération internationale dans le cadre de l'identification de cyberattaques, dont il est généralement difficile de trouver l'origine, sur la responsabilité de l'État à l'égard des cyberattaques lancées depuis leur territoire lorsque les États ne prennent aucune mesure pour y mettre un terme malgré qu'ils en sont informés et sur le devoir des États d'empêcher les zones de non-droit dans le cyberespace, telles que l'approbation, en connaissance de cause, du stockage de données personnelles collectées illégalement sur leur territoire.

Aspects militaires de la cybersécurité

La gestion de situations toujours plus complexes à tous les niveaux de commandement nécessite un recours accru aux technologies de l'information par les forces militaires. C'est pourquoi la protection et le traitement des informations sont devenus une mission de première importance.

Toutefois, d'un point de vue militaire, la sécurité de l'information est remise en cause non seulement par un adversaire potentiel, au niveau opérationnel, utilisant des armes pour détruire physiquement une infrastructure d'information, mais aussi par des utilisateurs irresponsables, des technologies défaillantes, des criminels ou simplement des accidents.

Par conséquent, des efforts doivent être consentis dans plusieurs domaines, de la sensibilisation de chaque utilisateur et de la garantie de la fiabilité de la chaîne logistique des technologies de l'information à la mise en place d'une défense adaptée pour contrer les cyberattaques ainsi que d'une architecture informatique globale résistante.

Il s'agit essentiellement d'assurer une gestion globale des risques et d'appliquer des mesures de renforcement de la sécurité de l'information à l'échelle nationale et mondiale.

Les forces armées allemandes (Bundeswehr) ont créé des architectures de commandement et de contrôle solides, des techniques et procédures de sécurité et une organisation dédiée à la sécurité des technologies de l'information englobant toutes les armes et comprenant une équipe d'intervention informatique d'urgence pouvant intervenir en cas de perturbations majeures des opérations informatiques. En outre, il convient d'adapter continuellement les capacités personnelles et techniques à la hausse perpétuelle du niveau de menace.

Les forces armées allemandes collaborent étroitement avec le Ministère allemand de l'intérieur et soutiennent fortement le renforcement de la sécurité de l'information au sein de l'Organisation du traité de l'Atlantique Nord (OTAN) et de l'Unions européenne et la définition de politiques et de capacités à cette fin. En outre, les forces armées allemandes procèdent régulièrement à des échanges avec plusieurs pays en matière de sécurité de l'information aux niveaux politique et opérationnel.

Les forces armées allemandes encouragent les initiatives et travaillent de concert avec d'autres départements du Gouvernement fédéral allemand dans le cadre des motions internationales visant à protéger davantage l'utilité des réseaux d'information au niveau mondial, en élaborant, par exemple, un code de conduite international volontaire dans le cyberespace.

Cyberdéfense à l'OTAN

La cybersécurité a été identifiée par l'OTAN comme étant l'un des principaux problèmes émergents en matière de sécurité. Selon le concept stratégique adopté par les chefs d'État et de Gouvernement au Sommet de l'OTAN, qui s'est tenu à Lisbonne en novembre 2010, « les cyberattaques risquent d'atteindre un seuil pouvant menacer la prospérité, la sécurité et la stabilité des États et de la zone euro atlantique.»

Les chefs d'État et de Gouvernement ont chargé le Conseil de l'Atlantique Nord, dans la Déclaration du Sommet, « d'élaborer, en s'inspirant notamment des structures internationales existantes et sur la base d'un réexamen de notre politique actuelle, une politique OTAN de cyberdéfense en profondeur d'ici juin 2011, et de préparer un plan d'action pour sa mise en œuvre ».

Comme première étape de l'élaboration de la nouvelle politique, les Ministres de la défense de l'OTAN ont adopté, en mars 2011, un document conceptuel sur la cyberdéfense :

Le document conceptuel met l'accent sur la protection des réseaux de l'OTAN et des réseaux nationaux des États Membres qui sont liés aux réseaux de l'OTAN ou qui traitent des informations de l'OTAN (y compris l'élaboration de principes et de critères communs visant à garantir un niveau minimum de cyberdéfense dans l'ensemble des États Membres). Afin de réduire les risques émanant du cyberespace au niveau mondial, l'OTAN envisage de coopérer avec des nations partenaires, des organismes internationaux pertinents tels que les Nations Unies et l'Union européenne, le secteur privé et le monde universitaire.

L'Allemagne approuve l'engagement de l'OTAN en matière de cybersécurité et soutient activement les discussions.

Cybersécurité à l'Organisation pour la sécurité et la coopération en Europe

L'Organisation pour la sécurité et la coopération en Europe se penche sur les questions relatives à la cybersécurité depuis plusieurs années. Lors du Sommet de l'OSCE qui s'est tenu en 2010 à Astana, les Chefs d'État et de gouvernement des 56 États participants de l'OSCE ont souligné qu'ils devaient parvenir à « une plus grande unité de vues et d'action pour faire face aux nouvelles menaces transnationales ». La Déclaration commémorative d'Astana classe les cybermenaces parmi les menaces transnationales émergentes.

L'Allemagne a participé activement à la conférence de l'OSCE sur une approche globale de la cybersécurité : exploration du rôle futur de l'OSCE, qui s'est tenue les 9 et 10 mai 2011 à Vienne. Lors de la conférence, des recommandations concrètes concernant les activités de suivi de l'OSCE ont été examinées.

L'Allemagne continuera à appuyer activement les discussions de l'OSCE visant à explorer le futur rôle de l'OSCE dans le domaine de la cybersécurité.

Australie

[Original : anglais]
[31 mai 2011]

L'Australie est heureuse de pouvoir présenter cette réponse contenant ses observations formulées comme suite à la résolution 64/41 de l'Assemblée générale sur les progrès de l'informatique et de la télématique et la question de la sécurité internationale.

L'Australie ambitionne de devenir le leader mondial de la cybersécurité. Elle reconnaît l'importance et les bénéfices des progrès technologiques pour l'économie numérique mondiale et la sécurité de toutes les nations. L'Australie envisage de tirer profit de son expertise pour optimiser les avantages en matière d'économie et de sécurité pour l'ensemble des nations.

Les technologies étant de plus en plus présentes dans notre quotidien, l'État, les entreprises et les individus en dépendent de plus en plus largement à des fins et fonctions diverses, allant des achats de produits et de services en ligne, de la communication avec autrui, de la recherche d'informations et de la gestion de ses finances au contrôle des équipements dans les industries minières et manufacturières. Afin de maximiser les avantages de l'Internet et de l'économie numérique et pour renforcer la cybersécurité au niveau mondial, il est impératif que les nations travaillent de concert à la mise en place d'un cyberespace fiable, sûr et résistant. L'Australie se veut un acteur proactif et engagé dans le renforcement du cyberespace pour l'ensemble des utilisateurs – État, entreprises et individus.

Problèmes généraux en matière de sécurité de l'information

L'Australie reconnaît que la cybersécurité constitue une priorité fondamentale en matière de sécurité nationale. La cybercriminalité observée par la communauté mondiale se veut toujours plus vaste, plus perfectionnée et plus efficace. Avec

l'augmentation de la quantité et de la valeur des informations électroniques, les criminels et autres protagonistes malintentionnés sur l'Internet ont pris davantage de mesures pour pouvoir exercer leurs activités de manière plus anonyme, plus pratique et plus rentable.

L'exposition à ces risques et leur gestion doivent être mesurées par rapport aux libertés civiles individuelles, y compris le droit à la protection de la vie privée, et la nécessité de promouvoir l'efficacité et l'innovation pour permettre à l'Australie de réaliser toute la mesure de l'économie numérique.

La sécurité nationale, la prospérité économique et le bien-être social de l'Australie et de chaque nation individuelle sont fortement tributaires de la disponibilité, de l'intégrité et de la confidentialité d'une série de technologies de l'information et des communications. En réaction, le Gouvernement australien a affecté des ressources considérables à la promotion proactive de la maintenance d'un environnement d'exploitation électronique fiable, sûr et résistant à l'intention de tous les utilisateurs.

Bien que l'accent de la politique du Gouvernement australien en matière de cybersécurité soit mis sur la disponibilité, l'intégrité et la confidentialité des technologies australiennes de l'information et des communications, une coordination est assurée avec d'autres politiques et programmes connexes, tels que la cybersûreté, axée sur la protection des personnes, en particulier les enfants, contre les contenus offensants, l'intimidation, le harcèlement ou la prédation en ligne à des fins d'exploitation sexuelle.

Efforts engagés au niveau national pour renforcer la sécurité de l'information et les activités de coopération internationale menées dans ce domaine

Initiatives nationales de renforcement de la sécurité de l'information

L'Australie reconnaît qu'une modélisation des meilleures pratiques au niveau national est nécessaire si elle veut promouvoir la coopération internationale en matière de cyberespace. L'Australie dispose d'une approche intégrée de protection et de renforcement de la cybersécurité, sous l'autorité du Gouvernement. En 2009, le Gouvernement a publié sa stratégie en matière de cybersécurité, qui expose la finalité et les objectifs généraux de la politique du Gouvernement australien à l'égard de la cybersécurité et fixe les priorités stratégiques sur lesquelles le Gouvernement australien devra se concentrer pour atteindre ces objectifs. La stratégie décrit également les actions et mesures fondamentales qui seront prises par le Gouvernement australien, au moyen d'un ensemble de travaux approfondis, pour répondre à ces objectifs stratégiques prioritaires.

La politique australienne en matière de cybersécurité vise à maintenir un environnement d'exploitation électronique fiable, sûr et résistant qui soutienne la sécurité nationale du pays et optimise les avantages de l'économie numérique. Les principales initiatives de la stratégie comprennent la constitution de deux organisations qui se renforcent mutuellement : une nouvelle équipe nationale d'intervention informatique d'urgence et un centre d'opérations de cybersécurité. Créée en 2010, l'équipe d'intervention informatique d'urgence constitue un point de contact unique qui fournit à tous les Australiens et entreprises australiennes des informations relatives à la cybersécurité et garantit à l'ensemble des internautes

australiens l'accès aux informations sur les cybermenaces, les vulnérabilités de leurs systèmes et les meilleures façons de protéger leurs technologies de l'information et des communications. L'équipe d'intervention informatique d'urgence entretient des relations de travail étroites avec les propriétaires et opérateurs d'importantes infrastructures et entreprises qui exploitent des systèmes notables pour l'intérêt national de l'Australie. Elle propose à ces entreprises des informations ciblées sur les menaces pour la cybersécurité et sur les vulnérabilités, afin de les aider à mieux protéger leur infrastructure des technologies de l'information et des communications. Le centre d'opérations, également établi en 2010, apporte au Gouvernement australien des informations provenant de toutes sources lui permettant de prendre conscience de la cybersituation et renforce sa capacité à faciliter les interventions opérationnelles en cas d'événements de portée nationale en matière de cybersécurité. Le centre identifie et analyse les cyberattaques complexes et aide à répondre aux cyberévénements dans les systèmes et l'infrastructure de l'État et du secteur privé fondamental.

Informer tous les Australiens sur les outils d'information et de confiance ainsi que sur les outils pratiques leur permettant de se protéger en ligne, et de veiller à ce qu'ils puissent les utiliser en toute autonomie constitue une priorité majeure de la stratégie. Celle-ci se fonde sur le principe de la responsabilité partagée selon lequel tous les utilisateurs, lorsqu'ils profitent des avantages des technologies de l'information et des communications, sont encouragés à prendre toutes les mesures raisonnables pour assurer la sécurité de leurs propres systèmes et à faire preuve de prudence lors de la communication et du stockage d'informations sensibles et sont tenus de respecter les informations et les systèmes des autres utilisateurs. Pour que les personnes puissent jouer un rôle actif dans la sécurité de l'information, il est essentiel qu'elles restent sensibles au cyberenvironnement et à ses risques et qu'elles les comprennent. À cette fin, l'Australie dispose d'un programme de sensibilité permanent qui propose un site Web d'informations en matière de cybersécurité dédié aux particuliers et aux petites entreprises en Australie, y compris ceux qui ne disposent que de connaissances et de compétences limitées dans ce domaine (voir www.staysmartonline.gov.au) ainsi qu'une semaine de sensibilisation à la cybersécurité, organisée en association avec des entreprises, des groupes de consommateurs et des organisations communautaires. La semaine de sensibilisation aide les Australiens à comprendre les risques pour la cybersécurité et à informer les particuliers et les petites entreprises sur les simples mesures à prendre pour protéger leurs informations personnelles et financières en ligne. Lors de la semaine nationale de sensibilisation à la cybersécurité de 2010, environ 150 agences gouvernementales, organisations industrielles et communautaires et organisations de consommateurs se sont associées pour organiser des événements et des activités aux niveaux local, régional et rural. En 2011, la semaine de sensibilisation a eu lieu du 30 mai au 4 juin.

Reconnaissant que la sécurité du cyberespace est une responsabilité partagée, le Gouvernement australien a collaboré de manière proactive avec l'*Internet Industry Association* (IIA) au développement d'un code volontaire et novateur de bonne pratique pour la cybersécurité destiné aux fournisseurs d'accès à Internet (l'i-code), qui a vu le jour en décembre 2010. Le code fixe un cadre homogène permettant aux fournisseurs d'accès à Internet australiens de mieux informer, éduquer et protéger leurs clients par rapport aux problèmes de cybersécurité. L'Australie a fait état de la bonne application du code et a partagé les leçons tirées

de l'élaboration de ce code dans le cadre de forums multilatéraux. Le code a été présenté au groupe de travail de l'Organisation de coopération et de développement économiques (OCDE) sur la sécurité de l'information et de la vie privée en décembre 2010, au groupe de travail sur les télécommunications et l'information de l'Association de coopération économique Asie-Pacifique (APEC) et à la Télécommunauté de l'Asie et du Pacifique. L'Australie souhaite partager ce code avec d'autres États, par des opérations bilatérales de renforcement des capacités et des forums multilatéraux, afin d'aider les autres États à mieux collaborer avec les fournisseurs d'accès à Internet et à responsabiliser ces fournisseurs en matière d'éducation et de protection des utilisateurs finaux.

Promotion de la coopération internationale

L'Australie accorde une priorité élevée à la coopération internationale en matière de cybersécurité. Au vu de la nature transnationale de l'Internet, qui implique que la cybersécurité ne peut être efficace que si elle est assurée par une action concertée à l'échelle mondiale, l'Australie a mis au point une méthode active, à plusieurs niveaux, en faveur de l'engagement international. Celle-ci prévoit, entre autres, l'engagement auprès de gouvernements et organismes étrangers, de manière bilatérale et par l'intermédiaire de forums multilatéraux, afin de contribuer à la promotion des meilleures pratiques internationales, de partager des expériences, de renforcer les capacités et de favoriser une approche mondiale coordonnée de la lutte contre les menaces pour la cybersécurité.

La participation de l'Australie à l'Organisation des Nations Unies implique le coparrainage de résolutions sur la création d'une culture mondiale de la cybersécurité et l'évaluation des efforts nationaux visant à protéger l'infrastructure informatique sensible ainsi que sur les progrès de l'informatique et de la télématique et la question de la sécurité internationale. L'Australie a également répondu à la résolution 64/211 de l'Assemblée générale en fournissant des informations sur les meilleures pratiques en matière de protection de l'infrastructure informatique sensible, y compris les technologies de l'information et des communications, dans l'optique de contribuer à l'amélioration de la cybersécurité au niveau mondial. L'Australie est membre de l'Union internationale des télécommunications (UIT) et contribue à des groupes d'études relevant des Secteurs de normalisation des télécommunications et de développement des communications. L'Australie finance les activités de renforcement des capacités du Secteur de développement dans la région de l'Asie et du Pacifique, en ce compris des initiatives en matière de cybersécurité. L'Australie contribue activement au groupe de travail de l'OCDE sur la sécurité de l'information et de la vie privée, qu'elle a présidé auparavant, et compte actuellement parmi les pays volontaires pour la participation à une analyse comparative des stratégies en matière de cybersécurité. L'Australie a participé de manière intégrante, en tant que chef de file, au développement et à la mise en œuvre de l'Accord Séoul-Melbourne relatif à la coopération entre les nations d'Asie et du Pacifique dans la lutte contre le spam et du Plan d'action de Londres, qui constitue le premier réseau d'application et de coopération actif dans la lutte contre le spam.

L'Australie entretient des relations de collaboration avec ses partenaires régionaux avec lesquels elle s'engage à travailler. Elle coopère étroitement au renforcement des capacités avec d'autres pays dans sa région afin de mettre en place un cyberespace fiable, sûr et résistant. L'Australie participe à des activités du groupe de travail sur les télécommunications et l'information de l'Association de

coopération économique Asie-Pacifique (APEC TEL) et au travail du Forum régional de l'Association des nations de l'Asie du Sud-Est (ASEAN) sur la cybersécurité. L'Australie est le responsable adjoint du Groupe de coordination de la sécurité et de la prospérité d'APEC TEL. Elle cherche actuellement à codiriger le noyau de lutte contre la cyberterrorisme et le crime transnational dans le cadre du plan de travail du Forum régional de l'ASEAN.

Sur le plan opérationnel, l'équipe d'intervention informatique d'urgence entretient des relations de travail étroites avec ses organisations nationales dans le monde. En Australie, l'équipe facilite le partage fiable et opportun des informations au niveau mondial, y compris les informations sur les menaces et la vulnérabilité, et y participe activement, afin de garantir une connaissance constante de l'état de la situation et une réponse mondiale cohérente et coordonnée aux menaces en ligne. L'équipe contribue activement aux initiatives de renforcement des capacités, en particulier dans la région Asie-Pacifique, y compris par son appartenance à l'équipe d'intervention informatique d'urgence de la région Asie-Pacifique. Reconnaissant que la sécurité de l'information n'est pas limitée géographiquement, l'équipe travaille aussi étroitement avec d'autres partenaires par le biais de sa participation au Forum des équipes de veille et de réponse aux incidents de sécurité informatique et au Réseau international de veille et d'alerte.

Mesures qui pourraient être prises par la communauté internationale pour renforcer la sécurité de l'information à l'échelon mondial

Tous les États, y compris l'Australie, doivent continuer à rechercher des mesures aussi bien traditionnelles qu'innovantes pour renforcer la sécurité de l'information. Le défi mondial de la cybersécurité nécessite un effort accru lors des forums multilatéraux pour renforcer la sécurité des réseaux interopérables. Des mesures doivent notamment être prises au sein des Nations Unies et de l'UIT, de forums régionaux tels que l'APEC et de groupes internationaux plus spécifiques, tels que le Forum des équipes de veille et de réponse aux incidents de sécurité informatique et le Réseau international de veille et d'alerte.

L'Australie soutient l'établissement de principes internationaux de comportement responsable dans le cyberespace, notamment en convenant d'une série de principes de comportement normatif dans le cyberespace destinés à améliorer la coopération internationale et à encourager la confiance dans le cyberespace et qui mèneront au développement de normes convenues à l'échelle internationale sur le cyberespace. L'Australie, en tant que membre de la communauté internationale, continuera à encourager le progrès dans ce domaine, au moyen de forums bilatéraux et multilatéraux, vers un cyberenvironnement plus sûr, plus résistant et plus fiable.

Les mesures particulières qui pourraient être prises par la communauté internationale pour renforcer la sécurité de l'information à l'échelon mondiale comprennent :

a) L'élaboration de normes mondiales, y compris l'approbation d'une série de principes internationaux de comportement normatif dans le cyberespace afin d'améliorer la coopération internationale et d'encourager la confiance;

b) L'extension des capacités du système juridique international à la lutte contre la cybercriminalité, y compris l'établissement d'une cohérence entre les

cadres juridiques (par exemple, une plus large adhésion à la Convention du Conseil de l'Europe sur la cybercriminalité, dont les exigences devraient être remplies par l'Australie avant la fin de l'année 2011) et le renforcement de la coopération en matière répressive afin de permettre aux pays de promulguer efficacement une loi nationale;

c) L'élaboration et la promotion de meilleures pratiques en matière de sensibilisation à la situation et d'alerte stratégique et de réaction aux événements, y compris la constitution d'une équipe d'intervention informatique d'urgence chargée de réaliser et de coordonner ces activités entre toutes les nations;

d) La mise en place d'initiatives de sensibilisation et d'activités de renforcement des capacités par des États possédant une solide expérience afin d'aider les États en développement à créer un cyberespace fiable, sûr et résistant dans l'intérêt de tous;

e) La mise au point d'une approche plus cohérente axée sur les partenariats avec l'industrie afin d'établir des lignes directrices concernant le comportement à adopter dans le cyberespace, par exemple, le code de bonne pratique australien de l'industrie de l'Internet.

Concepts internationaux pertinents

Le droit international existant fournit un cadre pour la protection des menaces à la sécurité de l'information provenant de divers acteurs. Plusieurs principes juridiques internationaux peuvent s'appliquer à l'utilisation du cyberespace, y compris les principes de l'égalité souveraine des États et de l'interdiction de l'usage de la force et des actes d'agression, ainsi que le droit international humanitaire. Une discussion plus approfondie s'impose entre les États, dans le cadre de forums internationaux et régionaux, afin de déterminer plus précisément l'étendue et l'applicabilité de ces principes et menaces émanant de la cybersphère.

États-Unis d'Amérique

[Original : anglais]
[7 juin 2011]

I. Introduction

Les technologies de l'information et des communications sont déterminantes pour le développement de tous les États Membres. Reliées entre elles pour créer un cyberespace, ces technologies contribuent à la mise en place d'une vision commune de la société de l'information telle qu'envisagée lors des Sommets mondiaux sur la société de l'information de 2003 et 2005. Les technologies de l'information et des communications contribuent aux tâches essentielles de la vie quotidienne, au commerce, à la prestation de biens et de services, à la recherche, à l'innovation, à l'entreprise et à la libre circulation de l'information entre les personnes, les organisations et les pouvoirs publics. Elles constituent un nouvel outil puissant en ce sens qu'elles permettent l'administration en ligne, favorisent le développement économique, facilitent la fourniture d'une assistance humanitaire et autorisent les actions d'infrastructures civiles essentielles ainsi que d'infrastructures de sécurité publique et de sécurité nationale. En outre, on ne saurait trop insister sur la

promesse de réduction des obstacles à la compréhension et à la coopération internationale que nous offrent les communications en réseau.

La dépendance vis-à-vis des technologies de l'information et des communications augmente, entraînant avec elle une hausse des risques qui y sont associés. De nombreux événements et activités divers, d'origine humaine ou naturelle, menacent le bon fonctionnement des infrastructures nationales essentielles et des réseaux mondiaux ainsi que l'intégrité des informations qui y sont acheminées ou conservées. Les menaces humaines sont de plus en plus nombreuses, évoluées et graves. Même si certaines trouvent leur source dans l'État, un grand nombre proviennent d'acteurs non étatiques et impliquent des activités criminelles ou terroristes. Les motivations sont multiples, du vol d'argent ou d'informations ou de la déstabilisation de concurrents au nationalisme et à l'étendue de formes traditionnelles de conflit étatique au cyberespace. Ces menaces visent aussi bien les personnes que les entreprises, les infrastructures nationales essentielles et les pouvoirs publics et ont de graves conséquences sur le bien-être et la sécurité de chaque nation et de la communauté internationale dans son ensemble.

Quelles que soient les mesures que les gouvernements prennent au niveau national pour protéger leurs réseaux d'information, une collaboration internationale sur les stratégies de réduction des risques liées aux technologies de l'information et des communications est essentielle pour garantir la sécurité de tous. Les gouvernements doivent être certains de la sûreté et de la solidité des réseaux qui soutiennent leur sécurité nationale et leur prospérité économique. Le potentiel de la révolution de l'information sera pleinement réalisé lorsqu'une infrastructure fiable des technologies de l'information et des communications aura été mise en place.

Cette tâche ne sera pas facile. En effet, la communauté internationale est confrontée à la difficulté de maintenir un environnement qui encourage l'efficacité, l'innovation, la prospérité économique et le libre-échange tout en assurant la sûreté, la sécurité, les libertés civiques et les droits à la vie privée. La difficulté de la tâche est accentuée par les caractéristiques uniques des technologies de l'information et des communications. Accessibles à tous, les réseaux sont souvent détenus et gérés par le secteur privé plutôt que par les pouvoirs publics. Contrairement aux armes traditionnelles, les outils informatiques destinés à nuire sont discrets et invisibles. Ils peuvent traverser les nations sans qu'il soit possible de déterminer l'origine ni l'identité de leur auteur, ni l'autorité sous laquelle il agit. De plus en plus, les acteurs non étatiques développent des capacités qui font craindre que les acteurs étatiques ou non étatiques recourent à des mandataires pour se livrer à des activités perturbatrices dans le cyberespace. Au vu de ces caractéristiques, les stratégies traditionnelles, telles que des mesures similaires à celles utilisées pour la maîtrise des armes, s'avèrent inefficaces en termes de contrôle ou de limitation des menaces et il convient, par conséquent, d'adopter de nouvelles méthodes créatives pour réduire les risques. Nonobstant la difficulté de la tâche, les États Membres doivent s'unir dans l'accomplissement de l'objectif commun, à savoir préserver et renforcer la contribution apportée par les technologies de l'information tout en assurant leur sécurité et leur intégrité.

Les tâches des États Membres poursuivent un double objectif : national et international. La sécurisation des infrastructures nationales d'information est une responsabilité que les gouvernements doivent assumer au niveau national, en coordination avec des acteurs concernés de la société civile. Parallèlement, les

actions nationales doivent être appuyées par une collaboration internationale sur les stratégies visant à remédier à la nature transnationale des diverses menaces à l'encontre des systèmes d'information en réseau. Cela requiert une coopération en matière de gestion et de réduction des incidents ainsi que d'intervention en cas d'incident; des enquêtes et poursuites pénales transnationales; des recommandations techniques visant à renforcer la solidité de la cyberinfrastructure et l'affirmation de normes comportementales, partagées par la communauté internationale et étayées par des mesures de confiance destinées à renforcer la stabilité et à réduire les risques de perception erronée.

II. Menaces, risques, vulnérabilités

Les menaces à l'encontre du réseau de systèmes qui constituent ensemble le cyberespace ainsi que les informations qui y sont véhiculées représentent l'un des graves défis mondiaux du XXI^{e} siècle. Par l'intermédiaire des technologies de l'information et des communications, les acteurs étatiques et non étatiques peuvent s'attaquer à des citoyens ordinaires, au commerce, à des infrastructures industrielles essentielles et aux pouvoirs publics. La convergence entre les technologies de l'information et des communications, l'Internet et d'autres infrastructures offre des possibilités sans précédent de paralyser les télécommunications, l'alimentation électrique, les oléoducs/gazoducs et les raffineries, les réseaux financiers et d'autres infrastructures essentielles.

Les caractéristiques uniques des technologies de l'information facilitent leur utilisation à des fins de perturbation et posent d'importantes difficultés aux gouvernements qui cherchent à réduire les risques. À l'inverse des technologies militaires traditionnelles, les pouvoirs publics n'ont pas le monopole des réseaux qui constituent le cyberespace, lesquels sont le plus souvent détenus et gérés par le secteur privé. Les technologies de l'information constituent en elles-mêmes une technologie largement répandue dont la nature intrinsèque ne se veut ni civile ni militaire et dont l'utilisation dépend exclusivement de la motivation de l'utilisateur.

Les outils logiciels utilisés à des fins de perturbation sont accessibles à tous, du moins dans leur version de base. Les personnes qui disposent des compétences requises pourront mettre au point des systèmes plus perfectionnés. De plus, ces outils évoluent rapidement pour intégrer les nouvelles vulnérabilités découvertes. De tels outils ne sont pas visibles dans le sens classique du terme, sont assez discrets, et peuvent comporter des « signatures » latentes qui peuvent être imitées facilement. De par la nature de l'Internet, des codes malveillants peuvent transiter par plusieurs territoires nationaux avant leur destination finale. L'identification de leur origine s'avère donc être un processus long et onéreux, qui requiert souvent une collaboration transnationale considérable. Même lorsque leur origine est découverte, l'identité de l'auteur ou des coauteurs peut demeurer imprécise. Par conséquent, les auteurs mal intentionnés peuvent agir et agissent en secret, en toute impunité, aux quatre coins virtuels du globe.

À ce problème de dissimulation de l'identité s'ajoute celui de la dissimulation du motif de l'intrusion dans le cyberespace. Des criminels et autres personnes ou groupes de personnes organisés peuvent agir dans le but de servir leurs propres intérêts mais peuvent également revêtir la qualité de mandataire d'acteurs étatiques ou non étatiques. L'absence d'identification fiable et rapide et la possibilité de

mystification peuvent créer un climat d'incertitude et de confusion pour les gouvernements, augmentant ainsi le potentiel d'instabilité de crise, les réactions inappropriées et la perte du contrôle de l'escalade pendant des cyberincidents majeurs.

Les principaux acteurs qui constituent ensemble une menace au fonctionnement fiable du cyberespace sont notamment :

Les criminels. Nombre d'outils malveillants sont le fruit d'initiatives entrepreneuriales de criminels et de pirates informatiques organisés. La complexité et la portée croissantes des activités criminelles soulignent le potentiel d'activités malveillantes dans le cyberespace qui entravent la compétitivité nationale, entraînent une érosion générale de la confiance en l'utilisation de l'Internet à des fins commerciales et paralysent même l'infrastructure civile. Le volume et la portée de telles activités augmentent.

Les États. De plus en plus de rapports publics isolés indiquent que les États développent et recourent à des moyens leur permettant d'étendre les formes traditionnelles de conflit étatique au cyberespace ou d'utiliser le cyberespace pour les mettre en œuvre. Toutefois, il est toujours difficile de trouver des preuves probantes concernant la source ou les intentions sous-jacentes aux événements dont on suppose généralement qu'ils sont commandités par l'État. Comme c'est souvent le cas, l'identité et la motivation de l'auteur ou des auteurs de l'infraction peuvent uniquement être déduits de la cible, des conséquences et d'autres indices entourant un incident.

Les terroristes. Actuellement, les terroristes n'ont pas les capacités de compromettre des réseaux d'informations ou de mener des opérations entraînant des conséquences physiques en se servant des technologies de l'information et des communications. Toutefois, l'éventualité que ces capacités puissent émerger à l'avenir ne peut être exclue. La plupart des experts conviennent que les terroristes se basent actuellement sur les technologies de l'information et des communications pour recruter, organiser leurs activités et solliciter des fonds. L'utilisation de l'Internet pour organiser et effectuer une attaque terroriste spécifique à l'aide d'armes à énergie cinétique peut constituer une menace particulière découlant de l'utilisation de l'Internet par des terroristes.

Les mandataires. Les personnes ou groupes qui participent à des activités malveillantes en ligne pour le compte d'autres acteurs étatiques ou non étatiques, à des fins lucratives ou nationalistes ou pour d'autres motivations politiques représentent une préoccupation croissante. Des pirates informatiques (appelés « botmasters ») offriraient divers services malveillants au candidat le plus offrant. Les caractéristiques uniques des technologies de l'information offrent un degré élevé d'anonymat à ces acteurs et rendent illisible toute relation avec un coauteur, ce qui offre à celui-ci la possibilité plausible de nier.

Les difficultés auxquelles sont confrontés les États dans la lutte contre de telles menaces sont considérables. Étant donné les caractéristiques des technologies de l'information et des communications, les actions de chacun de ces acteurs malveillants ne sont probablement visibles que dans leurs effets. Par conséquent, une identité hautement fiable ne peut être attribuée aux auteurs des crimes en temps opportun, voire jamais, et la réussite est souvent tributaire d'un degré élevé de collaboration transnationale. Le rôle croissant des mandataires complique le

processus d'attribution, étant donné qu'une partie lésée doit identifier l'auteur du délit mais également le coauteur, ce qui laisse présager que ce défi sera encore plus complexe à l'avenir.

De tels défis requièrent que les gouvernements nationaux organisent et entreprennent des efforts sur le plan national afin de mettre au point et de déployer des moyens de défense solides et en couches pour les infrastructures de communications et d'information, sans tenir compte de la source de la menace. En outre, la nature transnationale complexe de ces menaces exige une collaboration internationale en matière de stratégies de lutte contre les risques au niveau mondial.

III. Principes, règles et normes de comportement

A. Responsabilités des États en matière de garantie de la cybersécurité

Ces dernières décennies, les États Membres ont reconnu qu'il relevait de leur devoir national de prendre des mesures internes systématiques pour répondre aux menaces en matière de cybersécurité et ont affirmé la nécessité d'une coopération internationale. Cinq résolutions de l'Assemblée générale ont attiré l'attention sur les mesures défensives essentielles pouvant être prises par les pouvoirs publics pour réduire les risques pour leur sécurité. Bien que destinées à sensibiliser, ces résolutions proposent des normes utiles de comportement individuel et étatique au service de la cybersécurité :

a) La résolution 55/63 sur la lutte contre l'exploitation des technologies de l'information à des fins criminelles, dans laquelle l'Assemblée générale souligne la nécessité d'adopter une législation nationale moderne et efficace qui permette de poursuivre comme il convient la cybercriminalité et de faciliter une coopération transnationale immédiate en matière d'enquêtes;

b) La résolution 56/121, dans laquelle l'Assemblée générale note spécifiquement les travaux des organisations internationales consacrés à la lutte contre la criminalité faisant appel aux technologies de pointe, notamment ceux du Conseil de l'Europe pour élaborer la Convention sur la cybercriminalité.

Des travaux intenses ont été menés par les Nations Unies et d'autres organisations dans ce domaine. Les institutions des Nations Unies qui se consacrent principalement à l'utilisation de l'Internet à des fins criminelles comprennent notamment l'Office des Nations Unies contre la drogue et le crime, la Commission pour la prévention du crime et la justice pénale, le Congrès des Nations Unies pour la prévention du crime et la justice pénale et l'Union internationale des télécommunications;

c) La résolution 57/239 dans laquelle l'Assemblée générale affirme la nécessité de créer une culture mondiale de la cybersécurité, reconnaît qu'il incombe aux gouvernements de tenir compte de tous les éléments de société pour comprendre leurs rôles et responsabilités à l'égard de la cybersécurité et souligne les éléments complémentaires auxquels tous les acteurs de la société de l'information doivent s'attacher;

d) La résolution 58/199 dans laquelle l'Assemblée générale insiste en particulier sur les éléments à prendre en compte par les États Membres dans la création d'une culture mondiale de la cybersécurité et la protection des

infrastructures essentielles de l'information. Ces éléments peuvent également être considérés comme une série de normes auxquelles les gouvernements doivent se conformer et jettent les bases essentielles d'une collaboration internationale en matière de réduction des risques;

e) La résolution 64/211 dans laquelle l'Assemblée générale invite tous les États Membres à dresser un bilan détaillé des efforts nationaux qu'ils ont fourni pour renforcer leur cybersécurité, dans les domaines susmentionnés et dans d'autres domaines, en utilisant une méthode d'auto-évaluation décrite en annexe et à faire connaître leurs mesures et pratiques optimales susceptibles d'aider d'autres États Membres dans leurs efforts de cybersécurisation.

B. Normes applicables en cas d'hostilités

Malgré les caractéristiques uniques des technologies de l'information et des communications, les principes existants du droit international servent de cadre approprié à l'identification et à l'analyse des règles et normes de comportement devant régir l'utilisation du cyberespace dans le cadre d'hostilités. À cet égard, deux corpus de droits distincts mais interdépendants doivent être pris en compte : *jus ad bellum* (droit à la guerre) et *jus in bello* (droit dans la guerre). Le premier définit le cadre permettant de déterminer si un incident dans le cyberespace nécessite un recours à la force qui activerait le droit d'une Nation à la légitime défense. Le second définit le cadre permettant d'identifier les règles régissant l'utilisation du cyberespace en cas de conflit armé.

Jus ad bellum. Le cadre juridique régissant le recours à la force et à la légitime défense repose en grande partie sur trois dispositions de la Charte des Nations Unies :

a) L'article 2, paragraphe 4 de la Charte des Nations Unies prévoit que « tous les Membres s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État… »;

b) L'article 39 de la Charte habilite le Conseil de sécurité à constater l'existence d'une menace contre la paix, d'une rupture de la paix ou d'un acte d'agression et le charge de faire des recommandations ou de décider quelles mesures seront prises conformément aux articles 41 et 42 de la Charte;

c) L'article 51 de la Charte reconnaît et renforce le principe selon lequel « aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales. »

Il peut être difficile de déterminer définitivement, sur le plan juridique, si une activité perturbatrice dans le cyberespace constitue une agression armée activant le droit de légitime défense. Par exemple, dans le cas d'une menace dont l'auteur et les motifs sont inconnus, et dont les conséquences n'entraînent pas directement un décès ou une destruction physique, il est possible que les conclusions diffèrent quant à l'existence d'une agression armée. Toutefois, ces ambiguïtés et sujets de désaccord ne justifient pas la nécessité de définir un nouveau cadre réglementaire propre au cyberespace. Au contraire, ils reflètent simplement la difficulté d'appliquer, dans de nombreux cas, le cadre existant fixé par la Charte. Néanmoins, il peut arriver qu'une

activité perturbatrice dans le cyberespace constitue une agression armée. Dans ce cas, il convient d'appliquer les principes établis suivants :

a) Le droit de légitime défense dans le cadre d'une agression armée imminente ou effective s'applique à tout agresseur, qu'il s'agisse d'un acteur étatique ou non étatique;

b) Le recours à la force en cas de légitime défense doit se limiter à ce qui est nécessaire pour répondre à une agression armée imminente ou effective et doit être proportionnel à la menace considérée;

c) Les États sont tenus de prendre toutes les mesures nécessaires pour garantir la non-utilisation de leur territoire par d'autres acteurs étatiques ou non étatiques dans l'objectif d'y mener des activités armées, y compris la planification, la menace ou la perpétration d'agressions armées ou la fourniture d'une aide matérielle à cet égard, à l'encontre d'autres États et de leurs intérêts.

Jus in bello. Le droit des conflits armés fixe les règles, dénommées *jus in bello,* qui s'appliquent à la conduite des conflits armés, y compris celles régissant l'utilisation d'outils informatiques dans le cadre d'un conflit armé. Les principes clés suivants devraient notamment jouer un rôle important dans la détermination de la légalité des cyberattaques pendant un conflit armé :

a) Le principe de *distinction* exige que les attaques soient limitées aux objectifs militaires légitimes et que les biens civils ne soient pas soumis à des attaques;

b) L'*interdiction des attaques sans discrimination* comprend une interdiction des attaques qui utilisent un moyen ou une méthode de guerre ne pouvant raisonnablement pas être dirigé(e) contre un objectif militaire déterminé;

c) Le principe de *proportionnalité* interdit les attaques susceptibles de causer des pertes accidentelles de vies civiles, des blessures aux civils ou des dommages aux biens civils qui seraient excessifs par rapport à l'avantage militaire concret et direct visé.

Ces principes interdisent les attaques contre des infrastructures purement civiles dont l'arrêt des services ou la destruction ne générerait aucun avantage militaire significatif. En outre, le potentiel de dommages indirects devra être évalué avant d'attaquer une cible militaire. En d'autres termes, une analyse du ciblage, telle que traditionnellement effectuée dans le cadre d'attaques aux armes à énergie cinétique (conventionnelles et stratégiques), devra être réalisée dans le cadre des attaques informatiques.

Bien que les principes susmentionnés soient bien établis et qu'ils s'appliquent au cyberespace, il est également vrai que l'interprétation de ces corpus de droit dans le cadre d'activités dans le cyberespace peut présenter de nouveaux défis uniques qui nécessiteront une consultation et une coopération entre les nations. Ce n'est pas inhabituel. Le développement de nouvelles technologies rend souvent l'application des corpus de droit existants délicate.

C. Utilisation de mandataires

L'utilisation de mandataires pour mener des opérations perturbatrices constitue un exemple de domaine dans lequel les caractéristiques uniques des technologies de

l'information présentent de nouveaux défis pour les États. Le recours à des mandataires augmente considérablement les capacités de l'auteur et lui offre une possibilité plausible de nier. Bien que le droit international existant comprenne des dispositions régissant l'utilisation de mercenaires, l'utilisation de mandataires dans le cyberespace soulève de nouveaux problèmes de taille aux vastes répercussions. Les États devront travailler de concert à l'élaboration de solutions efficaces à ce problème.

D. Responsabilité d'autoriser la libre circulation de l'information

Les droits à la liberté d'expression et à la libre circulation de l'information figurent dans la Déclaration universelle des droits de l'homme et les Pactes internationaux relatifs aux droits civils et politiques, qui prévoient en des termes généraux, sous réserve de certaines limitations, que tout individu a droit à la liberté d'expression, ce qui englobe le droit de ne pas être inquiété pour ses opinions et celui de rechercher, de recevoir et de répandre, sans considération de frontières, les informations et les idées par quelque moyen d'expression que ce soit. Ces principes ont été affirmés lors de nombreux forums internationaux, dont l'Assemblée générale, l'Union internationale des télécommunications et le Sommet mondial sur la société de l'information.

E. Responsabilité de lutter contre le terrorisme

Au moins 16 résolutions existantes du Conseil de sécurité exhortent les États à lutter contre le terrorisme. Ces obligations s'appliquent pleinement lorsque les terroristes ou les personnes qui facilitent les actes terroristes se servent du cyberespace pour recruter, recueillir des fonds, transférer de l'argent, se procurer des armes ou planifier des attaques. Tous les États sont tenus de communiquer les informations dont ils disposent sur les activités de financement, de recrutement, de planification et de facilitation en ligne à des fins terroristes et de prendre des mesures à leur encontre, tout en respectant la souveraineté d'autres États et leurs propres responsabilités d'autoriser la libre circulation de l'information.

IV. Mesures de transparence, de stabilité et de réduction des risques et de coopération

Tel qu'indiqué plus haut, les États Membres sont confrontés à la difficulté de gérer un environnement de la menace extrêmement varié et complexe. Ces dix dernières années, des efforts considérables pour lutter contre la menace de cybercriminalité ont été déployés à l'échelon international. Des mesures en faveur d'une formation aux enquêtes et poursuites en matière de cybercriminalité ont été prises au niveau de l'Organisation des États américains, de l'Association de coopération économique Asie-Pacifique, de la Communauté économique des États de l'Afrique de l'Ouest, de l'Union africaine et du Conseil de l'Europe, entre autres. Une vaste coopération internationale dans le domaine des enquêtes et poursuites de la cybercriminalité a pu être mise en place grâce à la Convention sur la cybercriminalité et aux efforts bilatéraux déployés entre les pays touchés. Elle s'avère toujours être le moyen le plus efficace pour gérer la menace que représentent les activités criminelles pour les technologies de l'information et des communications.

D'autres questions transnationales méritent une attention similaire, parmi lesquelles les risques de perception erronée imputables à l'absence d'une compréhension commune des normes internationales liées au comportement étatique dans le cyberespace, qui pourrait nuire à la gestion de crise en cas de cyberévénement majeur. Par conséquent, l'élaboration de mesures visant à renforcer la coopération et la confiance, réduire les risques ou améliorer la transparence et la stabilité est préconisée :

Mesures de transparence

- Échange de stratégies et de meilleures pratiques nationales en matière de cybersécurité (enseignements tirés);
- Échange de vues nationales sur les normes internationales régissant l'utilisation du cyberespace;
- Échange de structures organisationnelles nationales dédiées à la cybersécurité et de points de contact;

Mesures de stabilité et de réduction des risques

- Établissement ou amélioration de liens de communication et de protocoles connexes afin d'y intégrer les cyberincidents;
- Renforcement de la coopération pour faire face aux acteurs non étatiques organisés (criminels, terroristes, mandataires);
- Mise au point de procédures permettant l'échange régulier d'informations entre les équipes nationales d'intervention en cas d'incident lié à la sécurité informatique;

Mesures de coopération

- Aide au renforcement des capacités en matière de cybersécurité dans les nations moins développées.

Géorgie

[Original : anglais]
[1 juin 2011]

La Géorgie a commencé à accorder une attention particulière au problème de la sécurité de l'information après août 2008, lorsque le Fédération de Russie a lancé une lourde attaque visant à paralyser les services à l'encontre de la Géorgie.

Au vu de l'évaluation de ces événements et dans le cadre du développement rapide et à grande échelle de projets et services d'administration en ligne observé récemment, la sécurité de l'information est devenue l'un des aspects essentiels du principe de sécurité nationale. Ces dernières années, le Gouvernement de Géorgie a mené un certain nombre d'initiatives notables afin d'améliorer la réglementation de la sécurité de l'information.

En 2010, une entité juridique, la *Data Exchange Agency*, a été créée sous la tutelle du Ministère de la justice de Géorgie, lequel est directement responsable du développement et de l'application des politiques de sécurité de l'information dans le

secteur public. La création de la *Data Exchange Agency* s'accompagne de la mise au point, par le Gouvernement de Géorgie, du mécanisme institutionnel d'établissement coordonné de la sécurité de l'administration en ligne et de l'information.

La *Data Exchange Agency*, dans le cadre des fonctions qui lui ont été attribuées en vertu du droit et de sa propre charte, travaille de concert avec le Ministère de la justice de Géorgie à la poursuite et à l'introduction d'une politique de sécurité de l'information qui soit conforme à la norme ISO 27000. L'Agence coordonne également l'application et l'introduction de mécanismes ou de normes nécessaires à la sécurité de l'information dans le secteur public et le secteur industriel, notamment par l'exercice d'activités de différents niveaux d'importance. Parmi ces événements figure l'une des principales, à savoir la conférence annuelle géorgienne sur les innovations en matière de technologies de l'information dont l'ordre du jour est toujours lié à la sécurité de l'information et à la cybersécurité et qui vise, en soutien à la mission de l'Agence, à établir et mettre en œuvre la politique de sensibilisation du public aux problèmes en matière de sécurité de l'information et de cybersécurité.

En ce qui concerne la cybersécurité quotidienne, la *Data Exchange Agency* est responsable de la mise en place et de la gestion de l'équipe d'intervention informatique d'urgence, qui œuvre actuellement au sein de l'Agence à la gestion des incidents de sécurité de l'information dans le cyberespace géorgien. L'Agence supervise également le fonctionnement du réseau gouvernemental géorgien pour la sauvegarde de sa sécurité.

Dans le cadre de ses fonctions liées aux technologies de l'information et des communications, l'Agence se charge également d'augmenter les niveaux de l'enseignement professionnel (afin de former des experts en sécurité de l'information, entre autres), de préparer les propositions, de contrôler la sécurité et de délivrer les certificats de signature électronique. Eu égard à l'enseignement professionnel, l'Agence envisage d'exécuter une série de projets spécifiques, visant à assurer le niveau approprié d'enseignement professionnel, avec l'aide de donateurs internationaux (tels que l'Union européenne et la Banque mondiale). Quant à la sécurité de la signature électronique, l'Agence s'y attèlera dès l'émission aux citoyens de cartes d'identité électroniques (portant une signature électronique) par l'agence chargée de l'État civil.

Outre l'activité de la *Data Exchange Agency* qui constitue la principale agence de coordination en matière de sécurité de l'information, il convient de s'attarder sur d'autres initiatives menées actuellement par le Gouvernement géorgien, dans lesquelles la *Data Exchange Agency* est activement engagée :

a) Le groupe de travail d'experts, qui œuvre à la définition du plan d'action (défini concrètement à la partie suivante) et de la stratégie en matière de cybersécurité, a été constitué sous l'autorité du Conseil de sécurité nationale géorgien;

b) Un certain nombre d'initiatives législatives ont été mises au point, y compris la loi administrative et la loi régissant les secrets d'État, qui devraient être proposées au Parlement géorgien en 2011. Il convient de mentionner en particulier le projet de loi sur la sécurité de l'information actuellement élaboré par la *Data Exchange Agency* et qui sera présenté au Parlement pour examen en 2011;

c) En 2010, les Ministères géorgiens de la justice et des finances avec l'aide de l'Agence, ont mis au point des réglementations internes en matière de sécurité de l'information (politiques et lignes directrices), qu'ils introduisent actuellement. Des initiatives similaires devraient également être appliquées dans d'autres institutions gouvernementales.

Grèce

[Original : anglais]
[6 juin 2011]

Les problèmes en matière de sécurité de l'information sont traités de manière plus approfondie que par le passé. Des mesures de lutte contre les menaces inhérentes à la globalisation actuelle des réseaux et des systèmes sont prises en considération. Des mesures visant à préserver la libre circulation de l'information sont à l'étude et appliquées aux niveaux national et international.

Les principes nationaux et internationaux actuels sont suivis et examinés. Il convient de formuler des recommandations internationales dans le cadre de l'évaluation des risques. La problématique de la cybercriminalité doit être traitée. Les droits de souveraineté nationale en matière de sécurité de l'information doivent être protégés.

Tous les États Membres doivent continuer à communiquer au Secrétaire général leurs points de vue et de leurs observations sur les questions pertinentes. À cet égard, il convient de souligner les points suivants :

a) Toutes les questions en matière de sécurité de l'information sont hautement appréciées;

b) Des solutions visant à préserver la libre circulation de l'information et à garantir le niveau requis de confidentialité, d'intégrité et de disponibilité sont à l'étude et appliquées de part et d'autre des frontières nationales et internationales;

c) Il convient d'élaborer et de définir d'un commun accord des principes d'interconnexion de réseaux offrant des perspectives d'application et de partage aux niveaux national et international. L'estimation des risques eu égard à l'interconnexion des réseaux doit revêtir un caractère prioritaire et des lignes directrices internationales pertinentes doivent être formulées. En outre, comme la nécessité de prendre des mesures en faveur de la lutte contre la cybercriminalité constitue une source d'inquiétude importante pour toute nation, il convient de définir des lignes directrices cohérentes au niveau international dans une optique de coopération, d'efficacité et d'économie. Enfin, la nécessité pour une nation de préserver sa souveraineté et de disposer d'une base d'informations propre doit être prise en compte dans le cadre de l'élaboration de tout principe;

d) Mesures éventuelles devant être prises par la communauté internationale pour renforcer la sécurité de l'information à l'échelon mondial :

i) Présentation détaillée et définition commune des principes internationaux pertinents;

ii) Proposition d'un plan d'orientation pour une infrastructure globale harmonisée, couvrant les principales questions législatives afin d'offrir la

sécurité requise en matière d'information dans le cadre de la gestion électronique de la correspondance et de la messagerie, tout en assurant différents moyens de communication;

iii) Harmonisation et diffusion des principes adoptés dans le cadre d'alliances multinationales et de groupes de petites nations afin de les appliquer au niveau mondial. La conclusion d'un accord visant à spécifier la menace et ses effets négatifs pourrait avoir une portée plus grande que toute mesure de conception élaborée puisque celle-ci pourrait être exploitée par des personnes malveillantes;

iv) Par ailleurs, la souveraineté de la nation doit être comprise comme la référence de base dans le cadre de toute tentative de globalisation. Il convient d'élaborer un principe international pour la définition de passerelles d'échange d'informations, incluant des solutions reflétant le niveau d'intégration souhaité. Il devrait alors servir de guide dans tous les efforts déployés aux niveaux national, multinational et international.

Kazakhstan

[Original : russe]
[7 juin 2011]

L'équipe d'intervention informatique d'urgence a été créée au Kazakhstan en 2010 afin de garantir la cybersécurité des technologies de l'information et de la communication.

Les informations reçues des utilisateurs du réseau Internet kazakh relatives à la découverte, sur le domaine KZ ou sur un site d'hébergement kazakh, de virus, de codes de sécurité, de programmes pour la création de réseaux zombies et d'infractions à la législation (pornographie, violence, violation des droits d'auteur, etc.) sont envoyées au CERT pour analyse.

Pays-Bas

[Original : anglais]
[6 juin 2011]

Appréciation générale des questions relatives à la sécurité de l'information

Les Pays-Bas encouragent l'utilisation de technologies de l'information et des communications fiables et sûres ainsi que la protection d'un Internet ouvert et gratuit qui respecte les droits de l'homme. Des technologies de l'information et des communications sûres et fiables sont essentielles à notre prospérité et à notre bien-être et servent de catalyseur à un développement économique durable.

Bien que les technologies de l'information et des communications offrent des possibilités, elles rendent également notre société plus vulnérable. Une coopération internationale s'avère fondamentale en raison du caractère transfrontalier des menaces. De nombreuses mesures ne seront efficaces que si elles sont appliquées ou coordonnées au niveau international. À cet égard, les Pays-Bas attachent une grande

importance aux partenariats public-privé et à la responsabilité individuelle de la part de tous les utilisateurs de technologies de l'information et des communications.

Efforts engagés au niveau national pour renforcer la sécurité de l'information et les activités de coopération internationale menées dans ce domaine

Les Pays-Bas s'emploient, à l'échelle nationale et internationale, à créer un environnement numérique sûr. Au niveau national, en février 2011, le Gouvernement néerlandais a présenté une stratégie nationale de cybersécurité intitulée « Renforcement par la coopération ». En juillet 2011, dans le cadre de cette stratégie, le Gouvernement mettra en place un Conseil national de cybersécurité dans l'optique de garantir une approche concertée entre le secteur public, le secteur privé, les établissements universitaires et les organismes de recherche. Le Gouvernement établira également un centre national de cybersécurité chargé d'identifier les tendances et les menaces et de contribuer à la gestion des incidents et des crises. Le centre aura pour tâche majeure d'effectuer des analyses des cybermenaces en se fondant sur des informations provenant de secteurs publics et privés. Il comprendra l'équipe d'intervention informatique d'urgence existante.

Au niveau international, les Pays-Bas contribuent activement aux efforts déployés par l'Union européenne, l'OTAN, le Forum sur la gouvernance d'Internet, l'UIT et d'autres partenariats. Les Pays-Bas encouragent une coopération pratique entre les centres de cybersécurité (y compris les organisations des équipes d'intervention informatique d'urgence) et un renforcement du Réseau international de veille et d'alerte. La hausse rapide de la cybercriminalité requiert une application efficace pour renforcer la confiance dans la société numérique. À cet égard, l'objectif des Pays-Bas est d'encourager les enquêtes transfrontalières avec des autorités chargées de l'application des lois dans d'autres pays européens et au-delà. Les Pays-Bas sont partie à la Convention sur la cybercriminalité du Conseil de l'Europe et encouragent les autres pays à y adhérer.

Mesures qui pourraient être prises par la communauté internationale pour renforcer la sécurité de l'information à l'échelon mondial

Les Pays-Bas réalisent qu'il est important de poursuivre le dialogue sur l'élaboration de normes en matière de comportement étatique visant à garantir une utilisation sûre du cyberespace. Ils tiennent à contribuer activement à ce dialogue. Pour commencer, les Pays-Bas gagent sur un Internet ouvert qui encourage l'innovation, stimule la croissance économique et protège les libertés fondamentales.

Les Pays-Bas attachent une grande importance à l'implication du secteur privé et d'institutions intellectuelles dans ce dialogue et souhaitent partager leur expérience et leurs meilleures pratiques.

L'échange international intensif de connaissances et de renseignements entre les parties prenantes et les organisations est essentiel au renforcement de la sécurité et de la fiabilité du cyberespace. La cohérence dans l'application des cadres juridiques internationaux existants constitue un autre problème important qui mérite une attention internationale.