Nations Unies A/68/156/Add.1

Assemblée générale

Distr. générale
9 septembre 2013
Français
Original : anglais/arabe

Soixante-huitième session
Point 94 de l'ordre du jour provisoire*
Progrès de l'informatique et des télécommunications et sécurité internationale

Progrès de l'informatique et des télécommunications et sécurité internationale

Rapport du Secrétaire général

Additif**

Table des matières

* A/68/150.

** Les informations figurant dans le présent additif ont été reçues après la publication du rapport principal.

13-47546 (F) 101013 101013

II. Réponses reçues des gouvernements

Allemagne

[Original : anglais]
[25 juin 2013]

Ensemble des questions qui se posent en matière de sécurité informatique

La numérisation des interactions économiques, administratives et personnelles se poursuit et s'accélère, offrant des perspectives sans précédent, tant aux pays industrialisés qu'à ceux en développement. Dans le même temps, la dépendance croissante aux technologies de l'information et des communications crée des vulnérabilités et des failles systémiques. Elle s'accompagne également d'une interdépendance inédite de l'ensemble des acteurs, du particulier aux administrations, en passant par les entreprises. Les cyberattaques prennent aujourd'hui la forme d'activités malveillantes plus sophistiquées, comme les menaces persistantes avancées ou les logiciels malveillants très évolués, qui visent des cibles stratégiques. Guidées par la recherche de profits ou de renseignements visant à contrôler des biens, des systèmes ou des infrastructures d'importance cruciale, ces activités nuisent fortement aux gouvernements ainsi qu'à de nombreuses entreprises et organisations, y compris aux opérateurs d'importance vitale, et sont bien connues pour les difficultés qu'il y a à les détecter. L'innovation est si rapide qu'elle prend régulièrement de vitesse les tentatives de sécurisation des technologies existantes. En outre, la relative facilité avec laquelle on peut se procurer les outils et les procédés malveillants sur le marché noir ou non réglementé accroît les risques, contre lesquels les méthodes traditionnellement utilisées en matière de sécurité informatique ne peuvent protéger nos environnements actuels.

Des pirates hautement compétents consacrent des moyens techniques et financiers considérables à déceler des failles dans les systèmes informatiques et télématiques afin de les exploiter à leurs propres fins. La difficulté à identifier avec fiabilité les auteurs de cyberattaques, qui leur permet de mener des attaques imputables à d'autres, pose des risques supplémentaires en matière de sécurité, tant à l'échelon national qu'à l'échelon international, en particulier en raison des erreurs d'interprétation et d'appréciation qu'elle génère. Il arrive souvent que des intrusions visant à recueillir des renseignements aient, dans un premier temps, l'apparence d'intrusions à des fins de destruction, ce qui accroît les risques d'erreur sur les futures attaques et sur les violations qui peuvent les accompagner quant à l'interdiction d'employer la force dans les relations internationales.

L'ambiguïté qui prédomine quant aux règles s'appliquant au cyberespace accroît l'imprévisibilité qui règne en matière de sécurité de l'information.

Les systèmes de conduite des installations se sont révélés particulièrement vulnérables aux opérations informatiques malveillantes dans les infrastructures d'importance cruciale. Il existe des risques élevés de dommages collatéraux incontrôlables à l'échelle mondiale, y compris d'infection des systèmes de contrôle industriels susceptible d'avoir des effets destructeurs sur les infrastructures. Une seule cyberattaque contre des infrastructures de télécommunications centrales pourrait entraîner plus de perturbations à l'échelle mondiale qu'une attaque physique.

Indépendamment des capacités des divers États et de leur niveau de sécurité dans le domaine informatique, il n'est pas rare que ceux-ci diffèrent les mesures concrètes visant à augmenter leur résistance aux cybermenaces, voire les laissent totalement de côté, à cause de l'incertitude qui entoure les risques et les moyens de les prévenir efficacement, de la complexité et du caractère innovant des attaques numériques, et du voile de secret qui recouvre les incidents individuels.

Mesures prises au niveau national

Établi en 1991, le Bureau fédéral de la sécurité informatique (Bundesamt für Sicherheit in der Informationstechnik, BSI) a été le premier et principal prestataire de services centralisés de sécrité informatique mis à la disposition du Gouvernement fédéral. À ce titre, il définit des normes minimum de sécurité informatique à l'usage de l'administration fédérale et tient le fichier central des incidents informatiques. Il a par ailleurs vocation à donner des avis et des conseils impartiaux dans le domaine de la sécurité informatique. Le BSI compte un certain nombre de grandes réalisations à son actif, par exemple la Norme de gestion du dispositif de sécurité informatique (IT-Grundschutz), l'équipe d'intervention informatique d'urgence à l'intention des agences fédérales (CERT-Bund), la plateforme de gestion des incidents et d'échange d'information (mise en place en 1994) et l'équipe d'intervention informatique d'urgence à l'intention du citoyen (Buerger-CERT), créée en 2006 afin de servir, d'informer et de sensibiliser le grand public. Le BSI émet par ailleurs des alertes signalant les logiciels malveillants et les défauts de sécurité des produits et services informatiques, informe les parties concernées (dont les fournisseurs de matériel informatique et le grand public) et formule des recommandations au sujet des contre-mesures à prendre.

Le plan national 2005 de protection des infrastructures informatiques, qui s'adresse à la fois aux administrations publiques et aux industriels, a donné lieu à l'élaboration d'une stratégie en matière de cybersécurité, adoptée par le Gouvernement fédéral en février 2011 et qui vise à protéger les infrastructures critiques.

Depuis 2008, le Gouvernement allemand et les exploitants d'infrastructures critiques coopèrent dans le cadre d'un partenariat public-privé. Le Plan de protection des infrastructures critiques (UP KRITIS) a institué des groupes de travail qui étudient les différents aspects de la cybersécurité tels que la gestion des crises, les exercices de simulation et la disponibilité des services critiques.

Le Centre national de veille informatique (Nationales IT-Lagezentrum), qui est géré par le BSI, surveille la sécurité du cyberespace dans le pays et dans le monde afin de pouvoir repérer et analyser rapidement les principales menaces et de recommander des mesures de protection. En cas de crise, il élargit ses capacités en se transformant en un Centre national d'action contre les crises informatiques (Nationales IT-Krisenreaktionszentrum), capable de s'attaquer aux crises en cours et d'en couvrir tous les éléments nationaux, à savoir notamment les réseaux des services de l'État et les infrastructures critiques.

Conformément à la stratégie de 2011 en matière de cybersécurité, toutes les autorités gouvernementales confrontées au problème de la cybersécurité doivent coopérer étroitement et directement les unes avec les autres et avec le secteur privé au sein du Centre national de cyberdéfense (Nationales Cyber-Abwehrzentrum), géré et hébergé par le BSI.

En vertu de son mandat, le Conseil national de la cybersécurité (Nationaler Cyber-Sicherheitsrat), organe composé de secrétaires d'État, se penche sur les questions fondamentales de la cybersécurité et sur la position de l'Allemagne dans ce domaine. Il s'agit en l'occurrence de coordonner les politiques étrangères en matière de cybersécurité, y compris les dimensions de la politique étrangère, de la défense, des politiques économiques et de la sécurité.

Une plateforme de coopération et d'échange d'information a par ailleurs vu le jour à l'échelle nationale en octobre 2012 : L'Alliance pour la cybersécurité (Allianz für Cybersicherheit) facilite la coopération étroite entre les partenaires dans les domaines économique, universitaire et administratif et notamment entre des entreprises spécifiques d'intérêt public.

Le plan de protection des infrastructures critiques est en cours d'actualisation au terme de quatre années d'activité. Il sera ouvert à d'autres exploitants d'infrastructures critiques et instituera un certain nombre de nouveaux groupes de travail dans les secteurs d'importance critique. Il prévoit aussi d'établir des rapports de coopération avec la nouvelle Alliance pour la cybersécurité.

Compte tenu des interconnexions planétaires qui caractérisent le cyberespace, une action coordonnée au niveau international s'avère essentielle. Au sein de l'Union européenne et dans les organisations internationales, l'Allemagne défend donc vigoureusement le principe du renforcement de la cybersécurité tout en plaidant en faveur de la protection des bienfaits sociaux et économiques du cyberespace.

Compte tenu de l'interconnexion mondiale des technologies de l'information, l'Allemagne préconise dans sa stratégie en matière de cybersécurité l'élaboration de normes générales, non contentieuses et politiquement contraignantes concernant le comportement des États dans le cyberespace. Les normes devraient pouvoir convenir 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 et un espace publics. Nous devons donc considérer sa sécurité en termes de résistance des infrastructures ainsi que d'intégrité et de sécurité des données en cas de panne des systèmes. Étant donné que le cyberespace est un espace public, les États doivent en promouvoir la sécurité, en particulier à l'égard d'activités criminelles et malveillantes, en protégeant ceux qui choisissent d'utiliser des outils de validation pour contrer l'usurpation d'identité, et en assurant l'intégrité et la confidentialité des réseaux et des données.

Le cyberespace est par nature mondial. La garantie de cybersécurité, l'application des droits et la protection des infrastructures informatiques critiques exigent un effort considérable de la part des États, à la fois au niveau national et en collaboration avec les partenaires internationaux. L'Allemagne possède une culture nationale spécifique de coopération entre un très grand nombre d'équipes d'intervention informatique d'urgence (CERT) dans tous les organes économiques, universitaires et administratifs. Dans ce contexte, l'équipe qui épaule les agences fédérales (CERT-Bund) est un point de contact bien établi pour toutes ces autres équipes. Aux niveaux européen et international, la CERT-Bund coopère avec les autres CERT gouvernementales; le Forum des équipes de veille et de réponse aux incidents de sécurité est le plus grand réseau mondial d'interconnexion des CERT dans le cyberespace.

Sur cette toile de fond, l'Allemagne est disposée à travailler sur une série de normes régissant le comportement d'État à État dans le cyberespace, y compris notamment sur des mesures de renforcement de la confiance, de la transparence et de la sécurité, à signer par le plus grand nombre possible de pays. Elle a donc participé activement en 2012 et 2013 aux travaux du Groupe d'experts gouvernementaux chargé de continuer d'étudier « les risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information et des mesures collectives qui pourraient être prises pour y parer, y compris les normes, règles ou principes de comportement responsable des États et les mesures de confiance touchant à l'espace informationnel » (résolution 66/24 de l'Assemblée générale).

L'Allemagne a exposé les éléments éventuels d'un tel code de conduite en matière de normes internationales à la conférence de l'Organisation pour la sécurité et la coopération en Europe (OSCE) sur la cybersécurité qui s'est tenue les 9 et 10 mai 2011, à savoir :

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

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

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 de la réglementation internationale du cyberespace;
- Échange des points de vue nationaux sur les normes juridiques internationales applicables à l'utilisation du cyberespace;
- Mise en place et notification de points de contact;
- Mise en place de mécanismes d'alerte rapide et renforcement de la coopération entre les équipes d'intervention informatique d'urgence;
- Amélioration de la 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 pour agir contre les acteurs non étatiques;
- Aide au renforcement des capacités en matière de cybersécurité dans les pays en développement et élaboration de mesures volontaires d'aide à la sécurisation du cyberespace lors des grandes manifestations.

Dans le prolongement de ces propositions, l'Allemagne a présenté un mémoire au Groupe d'experts gouvernementaux des Nations Unies en juillet 2012. Nous nous félicitons vivement des recommandations formulées par les experts au sujet des normes, règles ou principes de comportement responsable des États et des mesures de confiance dans le cyberespace, ainsi que de l'importance accordée à l'approche multipartite de la cybersécurité.

En 2011 et 2012, l'Allemagne a soutenu des projets portant sur la cybersécurité internationale ainsi que les mesures de confiance et de sécurisation

prises par l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) et l'Institut de recherche sur la paix et les politiques de sécurité de l'Université de Hambourg. La première cyberconférence de Berlin tenue en décembre 2011 a ouvert le débat international sur la question des risques, des stratégies et des mesures de confiance en matière de cybersécurité mondiale. La deuxième cyberconférence de Berlin, en septembre 2012, était consacrée à l'Internet et aux droits de l'homme. L'une de ses principales conclusions a été que la sécurité, la liberté et le respect de la vie privée en ligne étaient des notions complémentaires. L'Allemagne a également soutenu la Conférence de l'UNIDIR sur la cybersécurité, qui s'est tenue à Genève les 8 et 9 novembre 2012 autour de la question des mesures de confiance au service de la cyberstabilité.

Nous estimons par ailleurs qu'il faut ouvrir un débat sur la coopération internationale dans le cadre de l'attribution des cyberattaques, dont il est généralement difficile de trouver l'origine, sur la responsabilité des États en cas de cyberattaques lancées depuis leur territoire s'ils ne font rien pour y mettre fin alors qu'ils en sont informés, et sur l'obligation faite aux États de ne pas faciliter la création de zones de non-droit dans le cyberespace, par exemple en tolérant sciemment le stockage de données personnelles collectées illégalement sur leur territoire.

Les 27 et 28 juin 2013, la troisième cyberconférence de Berlin, consacrée au thème intitulé « Garantir la liberté et la stabilité du cyberespace : rôle et pertinence du droit international » et organisée par le Ministère fédéral des affaires étrangères en coopération étroite avec l'Université de Potsdam, a fourni des évaluations juridiques de cyberopérations qui ne franchissent pas le seuil de l'agression armée et ne relèvent donc pas du droit des conflits armés. En vertu des normes et principes internationaux en vigueur, les États sont responsables des actes commis dans leur espace souverain par les individus qui portent atteinte à la sécurité et à la stabilité des technologies de l'information et des communications. Chaque État devrait réfléchir aux mesures à prendre pour contrer ou vaincre les cyberattaques lancées dans son espace souverain ou empruntant ses réseaux. Les États doivent répondre des cyberactivités internationales criminelles qui leur sont imputables, et notamment des actes de délinquance commis dans le cyberespace par des agents à leur solde agissant selon leurs ordres ou sous leur supervision et leur contrôle, conformément aux normes en vigueur de responsabilité de l'État en vertu du droit international coutumier. Les États devraient prendre toutes les mesures nécessaires pour garantir que leur territoire n'est pas utilisé par d'autres États ou des acteurs non étatiques à des fins d'utilisation illégale des technologies de l'information et des communications dirigée contre des États tiers et leurs intérêts. Ces mesures indispensables devraient inclure la mise en place des cadres législatifs et réglementaires nationaux nécessaires pour s'acquitter des responsabilités internationales. Les cyberactivités internationales malveillantes peuvent porter préjudice aux États de trois manières : 1) les pays d'origine de la cyberactivité malveillante en subissent les effets dommageables; 2) les pays de transit voient leurs infrastructures informatiques être instrumentalisées à des fins de cyberactivité malveillante; 3) les pays cibles subissent les dommages causés par la cyberactivité malveillante. Dans tous ces cas de figure, les États sont tenus de prendre les mesures qui s'imposent; elles peuvent être matérielles ou concerner la procédure et vont de la prévention dans la période précédant le dommage potentiel à l'endiguement au moment du démarrage de la cyberactivité dommageable puis au suivi une fois que la cyberactivité malveillante a été contrée.

La cybersécurité à l'Organisation pour la sécurité et la coopération en Europe

L'Organisation pour la sécurité et la coopération en Europe (OSCE) s'intéresse depuis plusieurs années au problème de la cybersécurité. Lors de son sommet de 2010, qui s'est tenu à Astana, les chefs d'État et de gouvernement des 56 États participants ont souligné qu'ils devaient parvenir à « une plus grande unité de vues et d'action pour faire face aux nouvelles menaces transnationales ». Dans la Déclaration commémorative d'Astana, les cybermenaces figurent parmi les nouvelles menaces transnationales.

L'Allemagne a participé activement à la conférence de l'OSCE sur une approche globale de la cybersécurité, qui s'est tenue à Vienne en 2011, autour du thème « Explorer le futur rôle de l'OSCE ». Il a été question, lors de cette conférence, de formuler des recommandations concrètes concernant les activités de suivi de l'OSCE. Un groupe de travail informel a été créé en mai 2012 conformément à la décision 1039 (PC.DEC/1039) du Conseil permanent pour élaborer une série d'ébauches de mesures de confiance destinées à renforcer la coopération interétatique, la transparence, la prévisibilité et la stabilité, ainsi qu'à réduire les risques de malentendu, d'escalade et de conflit pouvant découler de l'utilisation des technologies de l'information et des communications. L'Allemagne a présenté à ce groupe, en juin 2012, un document officieux dans lequel elle suggérait l'adoption d'une première série de mesures de confiance dans le cadre de l'OSCE. Elle déplore qu'il n'ait pas été possible, lors du Conseil des ministres de Dublin, en décembre 2012, de parvenir au consensus qui aurait permis d'adopter cette série de mesures, mais se félicite du fait que le groupe ait repris ses travaux en 2013.

L'Allemagne continuera de soutenir activement la réflexion que mène l'OSCE sur son rôle futur dans le domaine de la cybersécurité.

La dimension militaire de la sécurité informatique

À chaque échelon de commandement, la gestion de situations toujours plus complexes contraint les forces armées à recourir davantage à l'informatique, et la protection des informations et de ses moyens de traitement devient une mission primordiale.

Pour les militaires, toutefois, le danger peut non seulement émaner d'un ennemi éventuel utilisant concrètement ses armes pour détruire physiquement l'infrastructure informatique mais également résulter d'utilisations irresponsables, de défaillances techniques, d'actions criminelles ou simplement d'accidents.

Il convient donc d'agir sur plusieurs fronts, en sensibilisant chaque utilisateur, en garantissant la fiabilité de la chaîne logistique des technologies informatiques, en mettant en place des moyens de défense contre les cyberattaques et en mettant au point des systèmes solides.

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

Les forces armées allemandes (Bundeswehr) ont dès le début mis en place des structures de commandement et de contrôle et des techniques et procédures de sécurité solides ainsi qu'un système de sécurité informatique commun à toutes les

armes prévoyant une équipe d'intervention rapide indépendante capable d'agir en cas de perturbation grave du système. Il importera d'adopter les capacités humaines et techniques à un niveau de menace allant continuellement croissant.

Les forces armées allemandes collaborent étroitement avec le Ministère de l'intérieur et encouragent vivement le renforcement de la sécurité informatique au sein de l'Organisation du traité de l'Atlantique Nord (OTAN) et de l'Union européenne, ainsi que la définition de politiques en la matière, et préconisent à cet effet une meilleure coordination des moyens. Elles abordent en outre régulièrement la question avec un certain nombre de pays, aux niveaux politique et opérationnel.

Les forces armées allemandes se félicitent des initiatives adoptées et collaborent, avec d'autres ministères, aux travaux menés à l'échelon international pour renforcer la sécurité des réseaux informatiques mondiaux et, notamment, à l'élaboration d'un code de conduite international volontaire pour le cyberespace.

La cyberdéfense à l'OTAN

L'OTAN considère la sécurité informatique comme l'un des principaux nouveaux problèmes de sécurité. Selon le concept stratégique adopté par les chefs d'État et de gouvernement lors du sommet de l'OTAN, qui s'est tenu à Lisbonne en novembre 2010, les cyberattaques risquent d'atteindre un niveau si élevé qu'elles menaceront la prospérité, la sécurité et la stabilité des États et de la région euro-atlantique.

Comme il le leur était demandé dans la déclaration issue du sommet, les ministres de la défense de l'OTAN ont adopté pour l'Organisation, en juin 2011, une politique de cyberdéfense assortie d'un plan d'action que l'Organisation s'emploie sans relâche, depuis lors, à mettre en œuvre.

Cette politique met l'accent sur la protection des réseaux de l'OTAN et de ceux des différents pays membres qui leur sont reliés ou qui traitent des données utiles à la réalisation des principales activités de l'Organisation (telles que la définition de normes et principes communs visant à garantir un niveau de cyberdéfense minimal dans tous les pays membres). Afin de réduire les risques que fait planer le cyberespace sur la planète, l'OTAN a l'intention de coopérer avec les pays partenaires, les organisations internationales compétentes (comme l'Organisation des Nations Unies et l'Union européenne), le secteur privé et le milieu universitaire.

L'Allemagne se félicite de l'importance que l'OTAN accorde au problème de la cybersécurité et soutient activement la concertation dans ce domaine.

Arménie

[Original : anglais]
[5 juillet 2013]

La sécurité de l'information a été définie dans l'arrêté présidentiel n° NK-97 du 25 juin 2009. Englobant les systèmes d'information, de communication et de télécommunications, elle est garante en grande partie de la sécurité nationale. Le texte adopté prévoit d'évaluer dans leur ensemble les problèmes liés à la sécurité de l'information dans la République d'Arménie, les défis et menaces actuels en la matière, y compris leur origine et leurs particularités, ainsi que d'examiner les

moyens à mettre en œuvre pour les combattre dans les différentes sphères de la vie publique.

Un comité intergouvernemental a été créé afin de coordonner la mise en œuvre des programmes relatifs à la sécurité de l'information.

Par une décision datée du 25 février 2010, le Gouvernement arménien a approuvé la définition de la constitution d'une cybersociété. Dans ce cadre a été délimitée la notion de cybersécurité et créé le Conseil du cybergouvernement. L'annexe 4 définit les activités permettant de garantir la cybersécurité de l'État. Un comité d'État et un groupe d'experts ont été créés à cette fin.

Les mesures ci-après, prises à l'échelon national, visent à renforcer la sécurité de l'information.

Conformément au décret gouvernemental n° 479-N du 30 avril 2009, une station spéciale de télécommunications destinée à assurer la sécurité d'Internet a été créée et mise en service. Elle vise à sécuriser le téléchargement des informations institutionnelles et la connexion à Internet des systèmes d'information des organes de l'État.

Au début de 2012, le groupe d'experts a établi un projet de programme national portant sur la création d'un système de cybersécurité dans le pays, qui est actuellement examiné par le Gouvernement arménien.

En 2006, la République d'Arménie a ratifié la Convention sur la cybercriminalité, ouverte à la signature à Budapest la même année et, en 2012, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Le Service national de sécurité et la Police arménienne sont les organes gouvernementaux chargés d'appliquer les dispositions des conventions susmentionnées. À l'heure actuelle, le groupe intergouvernemental d'experts s'emploie à mettre la législation nationale en conformité avec ces dispositions.

La République d'Arménie développe une coopération dynamique en matière de cybersécurité dans le cadre de l'Organisation pour la sécurité et la coopération en Europe (OSCE). Elle participe actuellement aux négociations tenues par le groupe de travail informel en vue d'élaborer une série de mesures de confiance relatives à la cybersécurité. Elle a intégré une action assortie de sept actions subsidiaires concernant la cyberdéfense, dans son plan d'action de partenariat 2011-2013 qu'elle met en œuvre en coopération avec l'Organisation du Traité de l'Atlantique Nord.

Canada

[Original : anglais]
[3 septembre 2013]

S'appuyant sur les analyses et les recommandations figurant dans le rapport sur les progrès de l'informatique et des télécommunications et la sécurité internationale, établi par le Groupe d'experts gouvernementaux, le Canada soumet au Secrétaire général ses vues et ses observations concernant les questions ci-après :

1. Sécurité de l'information

Le Canada est préoccupé par les menaces réelles et grandissantes que suscitent les activités malveillantes sur Internet, et il est conscient que la recherche de solutions à ce problème passe par la coopération nationale, régionale et internationale.

Le Canada a un intérêt stratégique à maintenir ouvert le cyberespace, compte tenu de l'importance qu'il revêt pour la prospérité et la sécurité du pays et au regard de la démocratie et des droits de l'homme. Les secteurs privé et public canadiens ont tous deux besoin de s'appuyer sur une infrastructure de l'information sûre et solide pour mener à bien leurs activités quotidiennes. Les systèmes informatiques, ainsi que les connexions à Internet et aux réseaux, sont à la base des infrastructures essentielles du pays, notamment dans les secteurs de l'énergie, de la finance, des télécommunications et de la production, et des systèmes d'information institutionnels. Le bon fonctionnement de ces équipements conditionne notre mode de vie et la santé économique, politique et sociale du pays.

Échelon national

Depuis 1996, le Gouvernement canadien, conscient que les systèmes vitaux permettant le fonctionnement des infrastructures essentielles du pays peuvent être l'objet de cyberattaques et qu'il a un rôle déterminant à jouer dans leur protection, a pris les mesures qui s'imposaient. Après avoir analysé sa capacité d'évaluer et de réduire les vulnérabilités de ses infrastructures, il a élaboré et mis en œuvre une méthode globale de protection en nouant des partenariats et en surveillant et analysant les cyberattaques et les menaces dirigées contre les systèmes du Gouvernement fédéral. En 2010, il a publié sa stratégie nationale et son plan d'action pour la protection des infrastructures essentielles et, au début de cette année, son plan d'action 2010-2015 définissant la stratégie applicable en matière de cybersécurité, dont les objectifs sont de sécuriser les systèmes gouvernementaux, d'établir des partenariats aux fins d'assurer la sécurité des systèmes informatiques vitaux hors Gouvernement fédéral et de faire en sorte que les Canadiens naviguent en toute sécurité sur Internet.

Échelon international

Depuis 2007, le Canada est l'un des principaux contributeurs au programme de cybersécurité de l'Organisation des États américains (OEA), qui vise à aider les États des Amériques à prévenir et à suivre les cybermenaces, et à y remédier, en renforçant la planification et la coordination nationales, ainsi que la coopération régionale. Dans le cadre du programme de renforcement de ses capacités de lutte contre le terrorisme, il a aidé plusieurs États membres de l'OEA à élaborer leur propre stratégie nationale de cybersécurité et à intégrer le réseau panaméricain des équipes d'intervention en cas d'urgence liée à la cybersécurité, établi dans le cadre de l'OEA.

Depuis 2012, le Canada et d'autres États membres de l'Organisation pour la sécurité et la coopération en Europe ont œuvré à l'élaboration de mesures de confiance et de sécurité, faisant en sorte de réduire les risques de malentendu, d'escalade et de conflit pouvant découler de l'utilisation de l'informatique et des communications.

Dans le cadre de divers forums, dont le Groupe des Huit, l'Office des Nations Unies contre la drogue et le crime et l'Organisation des États américains, le Canada concourt également de manière active à des initiatives internationales visant à lutter contre la cybercriminalité. Il fait également partie du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, constitué pour 2012-2013.

2. Principes internationaux

Les traités internationaux existants et le droit international coutumier s'appliquent à l'utilisation que font les États de l'informatique et des communications, ce qui est essentiel au maintien de la paix et de la stabilité et à la promotion d'un environnement technologique ouvert, sûr, pacifique et facile d'accès. En ce qui concerne le cyberespace, ce sont la Charte des Nations Unies, le droit international des droits de l'homme et le droit international humanitaire qui font référence. Dans le dernier rapport du Groupe d'experts gouvernementaux, le Canada s'est félicité de constater que les États considéraient l'application du droit international au cyberespace comme un élément essentiel pour définir des règles et des principes favorisant un comportement responsable des États.

Le Canada considère également que la recherche de solutions aux problèmes de sécurité qui se posent dans le domaine de l'informatique et des communications doit aller de pair avec le respect des droits de l'homme et des libertés fondamentales, notamment le droit de ne pas être inquiété pour ses opinions, ainsi que les droits à la liberté d'expression, d'association et de réunion, et le respect de la vie privée. Le droit à la liberté d'expression figure à la fois dans la Déclaration universelle des droits de l'homme et dans le Pacte international relatif aux droits civils et politiques. Ces deux instruments disposent que les droits reconnus aux personnes doivent également être protégés en ligne, en particulier la liberté d'expression qui s'exerce sans considération de frontières et par tout moyen de son choix.

3. Propositions de mesures visant à renforcer la sécurité de l'information à l'échelle mondiale

Le Canada coopère étroitement avec ses partenaires internationaux, dont les principales organisations multilatérales et les associations du secteur privé, pour renforcer la sécurité de l'information sur les réseaux dont dépendent la bonne santé économique et la sécurité du pays. Il s'efforce également d'améliorer la collaboration et le partage d'informations avec quelques partenaires essentiels et dans le cadre d'organisations multilatérales chargées de veiller à la cybersécurité.

Le Canada a créé un nouveau dispositif qui lui permet de réagir de façon coordonnée à tout incident informatique grave et d'associer les propriétaires et les exploitants de ses infrastructures essentielles à l'élaboration et à la mise en œuvre de leur propre stratégie de protection du cyberespace.

De nombreux pays se déclarent intéressés par le renforcement de la cybersécurité et la prévention de la cybercriminalité. Le principal instrument international qui traite expressément de ce dernier problème est la Convention sur la cybercriminalité, que le Canada a signée en 2001. Également connu sous l'appellation de Convention de Budapest, ce document fournit des orientations sur l'élaboration de lois générales et de portée nationale en matière de lutte contre la cybercriminalité, et il sert de cadre à la coopération internationale entre États.

Japon

[Original : anglais]
[12 août 2013]

Observations générales sur la sécurité de l'information

Le Japon considère le cyberespace comme l'un des piliers de l'activité socioéconomique, dans le secteur public comme dans le secteur privé. En permettant à l'information de circuler librement, le cyberespace garantit la liberté d'expression, et favorise la croissance économique, l'emploi et le développement, ainsi que la démocratie et la protection des droits de l'homme. Le cyberespace est devenu un élément indispensable de la vie quotidienne et s'est imposé dans le monde entier.

Si l'on veut profiter pleinement des bienfaits du « côté positif » du cyberespace, il devient toutefois de plus en plus nécessaire d'en garantir la sécurité et de protéger le droit à la vie privée et les droits de propriété intellectuelle. Qui plus est, les cyberattaques constituent aujourd'hui une menace transnationale qui n'épargne aucune région de la planète. Elles revêtent des formes différentes et peuvent émaner d'entités diverses et venir du monde entier. Aucun pays ne pouvant faire face seul à l'augmentation de la cybercriminalité et des cyberattaques, il est indispensable de s'attaquer au problème collectivement, à l'échelon international, avec la participation des parties prenantes et des États concernés.

Le Japon œuvre à la construction d'un cyberespace sûr et fiable, en s'attachant tout particulièrement à garantir la libre circulation de l'information et la liberté d'expression, ainsi que le nécessaire équilibre entre protection de la vie privée et sécurité.

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

Efforts engagés au niveau national pour renforcer la sécurité informatique

Dans le contexte récent d'aggravation des risques liés au cyberespace, la cybersécurité est devenue une question importante pour la sécurité nationale et la gestion des situations de crise, pour la prospérité économique et sociale, et pour la protection et la tranquillité des citoyens japonais.

C'est pourquoi, en juin 2013, le Japon a élaboré une stratégie de cybersécurité pour la période 2013-2015. Dans le cadre de cette stratégie, il mettra en œuvre des mesures visant à améliorer la sécurité de l'information au sein des administrations et des infrastructures essentielles, ainsi que de renforcer sa capacité de réponse aux attaques cybernétiques.

Plus concrètement, cette stratégie prévoit les mesures suivantes : promotion du partage d'informations sur les attaques cybernétiques grâce à des partenariats public-privé; amélioration des compétences en sécurité informatique des administrations, du secteur privé et du public en général; sensibilisation aux problèmes de cybersécurité; renforcement par la coopération internationale des capacités de réponse aux cyberattaques; et renforcement de la contribution du Japon à l'élaboration de règles internationales dans le domaine de la cybersécurité.

Efforts engagés au niveau national pour renforcer les activités de coopération internationale

S'agissant de l'élaboration de normes internationales sur l'utilisation du cyberespace, nous devons commencer de toute urgence à mettre au point des règles de conduite réalistes et applicables visant à résoudre les problèmes actuels de façon juridiquement non contraignante, afin de faire face à l'évolution rapide des cybertechnologies. Le Japon continuera de prendre une part active à ces efforts dans les instances internationales concernées.

S'agissant des mesures de confiance, le Japon participe activement à des consultations bilatérales avec les États intéressés ainsi qu'à des dialogues régionaux, notamment dans le cadre du Forum régional de l'ASEAN, afin d'« accroître la transparence » et de « promouvoir le partage de l'information ». De plus, afin d'empêcher l'application de « trous » dans la sécurité du cyberespace, le Japon aide des pays en développement d'Asie, d'Océanie et d'Afrique à renforcer leurs capacités, par exemple en mettant sur pied et en renforçant des équipes d'intervention informatique d'urgence. Il renforce également le partage de l'information à l'échelle internationale en resserrant sa coordination avec les équipes d'intervention informatique d'urgence des autres États. Toutes ces mesures contribuent à renforcer la confiance des États concernés.

Principes visés au paragraphe 2 de la résolution 67/27

De l'avis du Japon, le droit international existant, notamment la Charte des Nations Unies et le droit international humanitaire, s'applique à l'utilisation du cyberespace. Compte tenu cependant des caractéristiques particulières des technologies de l'information et de la communication en réseau, il est nécessaire d'approfondir la réflexion sur les modalités d'application des différents principes et règles.

Étant donné le rôle important joué par le droit international comme garant de la stabilité et de la sécurité juridique au sein de la communauté internationale, nous considérons que le fait de définir et de préciser les modalités d'application du droit international existants au cyberespace compléterait utilement l'élaboration de normes internationales spécifiques pour le cyberespace et contribuerait à créer un cyberespace stable.

Mesures que la communauté internationale pourrait prendre pour renforcer la sécurité informatique à l'échelon mondial

Normes internationales relatives à l'utilisation du cyberespace

Il n'existe pas de normes internationales qui encadreraient les cyberattaques et le cyberespionnage dans les domaines de la sécurité et de l'économie ou dans le domaine social. L'utilité de normes juridiquement contraignantes dans le cyberespace n'est d'ailleurs pas prouvée à ce stade. Compte tenu de l'évolution rapide des cybertechnologies, il est difficile de savoir à quoi ressemblera le cyberespace de demain. Or il faudra fort longtemps pour parvenir à un consensus sur des normes juridiquement contraignantes. C'est pourquoi, en ce qui concerne le caractère juridique des futures normes, le Japon juge qu'il vaut mieux commencer par envisager la possibilité de règles générales de conduite non contraignantes.

Mesures de confiance

Si elles sont assez nombreuses, les mesures de confiance entre États peuvent favoriser l'élaboration de normes internationales, aussi la communauté internationale doit-elle continuer de les encourager. Pour ce faire, il est indispensable de promouvoir la transparence et le partage de l'information. L'ampleur des mesures qu'ils prennent en ce cas varie selon les États, celles-ci relevant de l'autorité de chacun. Il est donc nécessaire d'encourager le partage de l'information dans le cadre de structures régionales et mondiales, notamment sous les auspices de l'Organisation des Nations Unies.

Oman

[Original arabe]
[26 juin 2013]

Le Ministère des transports et des communications souhaite communiquer les informations ci-après concernant la résolution 67/27 de l'Assemblée générale intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale » :

1. Évaluation d'ensemble de la question de la sécurité de l'information

Il ne fait pas de doute que les progrès extrêmement rapides accomplis par les technologies de l'information et de la télécommunication se sont accompagnés d'une multiplication et d'une extension des risques et menaces, ainsi que d'un développement, au niveau international, des données et des moyens et techniques utilisés par les pirates informatiques. Au nombre des difficultés et obstacles les plus importants auxquels sont confrontés les États et les institutions dans ce domaine, on citera l'absence de culture de la sécurité de l'information et la connaissance insuffisante, voire l'ignorance du problème parmi les utilisateurs des technologies de la communication, le manque de cadres compétents et les disparités des législations qui régissent les transactions électroniques à l'échelle internationale. Aussi faudrait-t-il que les États redoublent d'efforts et renforcent leur coopération en vue de lutter contre les menaces et les dangers qui pèsent sur la sécurité de l'information, améliorent les moyens dont ils disposent pour faire face à ces risques, sensibilisent l'opinion mondiale au problème et échangent des informations et des compétences dans ce domaine.

2. Efforts déployés au niveau national en vue de renforcer la sécurité de l'information et de promouvoir la coopération internationale dans ce domaine

- Création, en 2002, d'une instance chargée de réglementer les télécommunications et, en 2006, d'une autorité des technologies de l'information, aux fins de réglementer les secteurs des télécommunications et des technologies de l'information;
- Promulgation d'une législation pertinente, sous la forme d'une loi sur les transactions électroniques, promulguée par décret royal n° 69/2008, et d'une loi sur la réglementation des télécommunications, promulguée par décret royal n° 30/2002;

- Création récente, dans le Sultanat d'Oman, du premier centre d'innovation en matière de cybersécurité pour la région des États arabes, qui relève de l'Union internationale des télécommunications (UIT) et du Partenariat multilatéral international contre les cybermenaces (IMPACT);
- Mise sur pied, en avril 2010, par le Centre national de cybersécurité, d'une Équipe nationale d'intervention en cas d'urgence informatique (OCERT);
- Le Sultanat d'Oman est membre, par le truchement de l'Autorité des technologies de l'information, de plusieurs organisations et organismes régionaux et internationaux compétents, dont l'Équipe d'intervention en cas d'urgence informatique de l'Organisation de la Conférence islamique (OCI-CERT), l'Équipe d'intervention en cas d'urgence informatique du Conseil de coopération du Golfe (CCG-CERT) et le Forum des équipes de veille et de réponse aux incidents de sécurité informatique (FIRST). Bon nombre d'institutions omanaises ont obtenu des certificats ISO (Organisation internationale de normalisation);
- Les institutions compétentes ont des stratégies permanentes de développement des secteurs de la communication et de l'information;
- Les autorités gouvernementales ont accès à toute une gamme de technologies et de programmes de sécurité de l'information;
- Création d'un centre de protection des réseaux gouvernementaux;
- Mise en place de services d'hébergement et de sites informatiques gouvernementaux protégés;
- Fourniture d'un appui technique dans le domaine de la sécurité de l'information;
- Adoption d'une série de politiques et de normes relatives à la sécurité de l'information;
- Tenue d'une série de sessions de formation consacrées à la sécurité de l'information;
- Organisation d'une série de programmes et de campagnes de sensibilisation à la sécurité de l'information;
- Exécution de programmes visant à évaluer la préparation des interventions à mener en cas d'urgence informatique;
- Organisation de plusieurs ateliers et conférences régionaux et mondiaux sur la sécurité de l'information;
- Présence lors des activités et manifestations organisées au niveau local en vue de sensibiliser l'opinion au problème de la sécurité de l'information;
- Participation de tous les segments de la société aux efforts menés dans le domaine de la sécurité de l'information;
- Lancement, en janvier 2012, d'un forum dans le cadre du programme des Ambassadeurs de la sécurité informatique de l'OCERT;
- Création d'un site Internet pour la protection des enfants (cop.cert.gov.om);
- Organisation de visites de sensibilisation dans les écoles, les universités, les cafés Internet et autres lieux fréquentés par les jeunes;

- Tenue d'ateliers sur la sécurité de l'information visant à mieux sensibiliser les élèves et le personnel enseignant à la question;
- Participation active de l'OCERT à de nombreuses manifestations publiques en vue d'atteindre le plus grand nombre de jeunes possible et de leur faire connaître les risques pour la sécurité et les pratiques suivies pour les prévenir;
- Actualisation du programme de « formation de formateurs » au moyen duquel l'OCERT s'emploie à doter les jeunes cadres omanais des compétences voulues en matière de sécurité de l'information;
- Ouverture du premier centre d'opérations pour la sécurité de l'information à l'échelle du Moyen-Orient;

3. Teneur des principes

- Le Sultanat d'Oman surveille en permanence et étudie la teneur de ces principes internationaux, et ce, afin de se tenir au courant des efforts visant à renforcer la sécurité des systèmes d'information et de télécommunications mondiaux;
- Il faut tenir compte des spécificités des pays et de leur législation sur les transactions;
- Il importe de respecter les valeurs et les principes que chaque pays tient à conserver d'une manière qui soit adaptée à chaque pays;

4. Mesures qui pourraient être prises par la communauté internationale pour renforcer la sécurité de l'information à l'échelle mondiale

- Réglementer les transactions électroniques et la cybersécurité dans le domaine de l'informatique et des télécommunications interétatiques en créant un organisme international relevant de l'Organisation des Nations Unies, comme cela a été proposé à la Conférence sur la cybersécurité qui s'est tenue dans le Sultanat d'Oman en mars 2013;
- Promouvoir la coopération entre les États afin d'assurer la sécurité du secteur des technologies de l'information et de la communication qui, dans la plupart des pays, est aujourd'hui, dans une large mesure, un moteur essentiel du développement. Ces efforts de coopération doivent être menés sous les auspices d'une organisation internationale;
- Poursuivre les efforts de coordination entre États en vue de renforcer la sécurité de l'information et de permettre l'examen des expériences novatrices menées dans ce domaine;
- Coopérer dans le domaine de la lutte contre les atteintes à la sécurité de l'information et nommer, dans chaque pays, des points de contact auxquels on puisse en faire appel en cas d'incident de cette nature;
- Participer à l'application de politiques, de règlements et de pratiques optimales en matière de sécurité de l'information;
- Participer aux programmes d'acquisition de compétences et de connaissances spécialisées dans le domaines suivants : cybersécurité et visites d'échange;
- Organiser des colloques et des ateliers à l'intention du personnel chargé de la sécurité;

- Organiser des programmes internationaux conjoints visant à mieux faire connaître la culture de la sécurité de l'information et à en promouvoir la diffusion;
- Promouvoir la collaboration entre universitaires ainsi que l'élaboration de programmes et de curriculums pertinents;
- Encourager et promouvoir les programmes de recherche-développement conjoints dans les domaines précités.

Pays-Bas

[Original : anglais]
[7 août 2013]

Les Pays-Bas se félicitent de la possibilité qui leur est donnée de donner suite à la demande formulée par l'Assemblée générale dans sa résolution 67/27.

Ensemble des questions qui se posent en matière de sécurité informatique

Les Pays-Bas défendent des TIC sûres et fiables, ainsi qu'un Internet ouvert, libre et respectueux des droits de l'homme. Ces éléments, indispensables à notre prospérité et à notre bien-être, sont également les catalyseurs d'une croissance économique durable.

Si le cyberespace offre de multiples possibilités, il expose également nos sociétés à davantage de risques. Étant donné le caractère transfrontalier des menaces, la coopération internationale est fondamentale. Bien des mesures ne seront efficaces que si elles sont appliquées ou coordonnées à l'échelle internationale. À cet égard, les Pays-Bas attachent une grande importance aux partenariats public-privé, aux mesures de confiance propices aux rapprochements, ainsi qu'à la sensibilisation de chacun à sa responsabilité individuelle en tant qu'utilisateur des TIC.

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

Tant sur le plan national que sur le plan international, les Pays-Bas s'emploient à créer un environnement numérique sûr. Au niveau national, le pays met en œuvre sa stratégie de cybersécurité, intitulée « Renforcement par la coopération », qu'il actualisera en 2013 en prévision d'une publication au second semestre. Cette nouvelle version portera sur le cyberespace dans son ensemble du point de vue notamment des avantages économiques, de l'ouverture et des libertés, et de la sécurité.

Les Pays-Bas ont mis en place un Conseil national de la cybersécurité afin de garantir une approche concertée entre le secteur public, le secteur privé, les établissements universitaires et les organismes de recherche, et de conseiller les décideurs dans le domaine de la cybersécurité. Ils disposent également d'un Centre national de la cybersécurité, qui identifie les tendances et les menaces et contribue à la gestion des incidents et des crises, avec trois tâches principales : analyser les cybermenaces sur la base d'informations provenant des secteurs public et privé; répondre aux cybermenaces et aux incidents; et coordonner les opérations en cas de crise liée aux TIC. Pendant l'année écoulée, le Centre, dont dépend l'équipe d'intervention informatique d'urgence du Gouvernement, a développé ses capacités

et établi des relations étroites avec d'importants centres d'analyse et de partage de l'information. Il organise en outre chaque année une conférence internationale qui réunit des experts envoyés par les États, le secteur privé et les services de police ainsi que des spécialistes des technologies concernées pour qu'ils échangent des bonnes pratiques. Les Pays-Bas ont mis en œuvre des mesures importantes pour améliorer la cybersécurité et ils sont plus que disposés à transmettre à d'autres États les modèles dont ils se sont inspirés.

Comme exemple de partenariat public-privé appliqué au secteur de la sûreté nucléaire, on peut citer les réunions techniques organisées par le Gouvernement, qui ont permis à l'industrie nucléaire de lui faire connaître ses besoins en matière de sécurité informatique. Les données recueillies ont ensuite été exploitées pour mieux définir la « menace de référence », les mots clefs étant ici « réalisme » et « proportionnalité ».

Au niveau international, les Pays-Bas contribuent activement aux efforts déployés par l'Union européenne, l'Organisation du Traité de l'Atlantique Nord (OTAN), l'Organisation pour la sécurité et la coopération en Europe (OSCE), le Forum sur la gouvernance d'Internet, ainsi qu'à ceux déployés dans le cadre d'autres partenariats. Ils saluent la communication conjointe, approuvée par le Conseil européen, dans laquelle la Commission européenne et la Haute Représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité appellent à la création d'un cyberespace ouvert, libre et sûr au sein de l'Union européenne. L'Union européenne a entrepris de relever ce défi en collaboration avec ses partenaires internationaux, les organisations internationales, le secteur privé et la société civile. Les Pays-Bas soutiennent sans réserve les objectifs que l'Union européenne s'est fixés de garantir un Internet sûr tout en favorisant son ouverture et sa liberté, d'encourager la mise en place de mesures de confiance et de règles de conduite, et d'appliquer au cyberespace le droit international en vigueur. Nous sommes fermement convaincus que la sécurité et le droit d'accès sont des éléments essentiels pour assurer la continuité du développement d'Internet. Pour ce faire, l'Union européenne s'est donné pour principes directeurs les valeurs fondamentales que sont la dignité humaine, la liberté, la démocratie, l'égalité, la primauté du droit et le respect des droits fondamentaux. Les Pays-Bas souscrivent à ces valeurs, dans lesquelles ils voient les fondements de toute stratégie de cybersécurité. Ils reconnaissent que, pour promouvoir un cyberespace solide et résilient, les secteurs public et privé doivent tous deux développer leurs capacités et collaborer efficacement.

Au niveau opérationnel, les Pays-Bas encouragent une coopération concrète entre les centres de cybersécurité (notamment les équipes d'intervention informatique d'urgence) et un renforcement du Réseau international de veille et d'alerte. L'augmentation rapide de la cybercriminalité exige des mesures de répression efficaces si l'on veut maintenir la confiance dans la société numérique. À cet égard, les Pays-Bas encouragent les enquêtes transfrontalières avec les autorités de police d'autres pays européens et d'ailleurs. Partie à la Convention sur la cybercriminalité du Conseil de l'Europe, les Pays-Bas encouragent les autres États à y adhérer.

S'agissant de la sécurité informatique de l'industrie nucléaire, les Pays-Bas communiquent des informations sur leurs politiques et sur leurs bonnes pratiques en matière de sûreté nucléaire et de cybersécurité dans le cadre de l'ENSREG (Groupe des autorités de sûreté nucléaire européennes). En outre, ils participent activement

aux réunions techniques qu'organise l'Agence internationale de l'énergie atomique pour promouvoir l'échange de renseignements en matière de cybersécurité et de sécurité informatique.

Convaincus que la liberté, la transparence et la sécurité sont interdépendantes et se renforcent mutuellement, les Pays-Bas ont lancé l'initiative de la Coalition pour la liberté en ligne, aujourd'hui forte de 21 gouvernements membres. Créée pour promouvoir la liberté sur Internet et défendre les droits humains de ses usagers, la Coalition réunit des gouvernements qui, attachés aux libertés et aux droits fondamentaux, coordonnent leurs efforts et collaborent avec la société civile et le secteur privé afin de défendre l'aptitude de tout un chacun à exercer ces droits et jouir de ces libertés sur Internet. Afin de faire avancer la cause d'un Internet libre et ouvert à tous, ses membres ont créé un partenariat de défense des libertés d'Internet (Digital Defenders Partnership), fonds destiné à appuyer des solutions innovantes pour assurer la protection des blogueurs et des militants en ligne ainsi qu'à déployer des services Internet d'urgence dans les pays où celui-ci, ou son accès, n'est pas libre. Les Pays-Bas ont contribué à ce fonds à hauteur de 1 million d'euros pour la période allant du 1er octobre 2012 au 31 décembre 2014.

Mesures que la communauté internationale pourrait prendre pour renforcer la sécurité informatique à l'échelon mondial

Les Pays-Bas gagent sur un Internet ouvert qui encourage l'innovation, stimule la croissance économique et protège les libertés fondamentales. Ils soulignent qu'il importe de poursuivre le dialogue sur l'élaboration de règles de conduite applicables aux États qui garantiront une utilisation sûre du cyberespace, dialogue auquel ils tiennent à participer activement. Les Pays-Bas se félicitent des efforts importants déployés par divers acteurs et parties prenantes aux échelons régional et international, notamment le Conseil de l'Europe, l'Union européenne, l'OSCE et le Groupe d'experts gouvernementaux des Nations Unies, pour développer des mesures de confiance dans le domaine de la cybersécurité.

La sécurité informatique joue un rôle central dans le contexte du Sommet sur la sécurité nucléaire. Le plan de travail issu du Sommet de Washington et le Communiqué de Séoul affirment tous deux que les États participants visent à empêcher que des acteurs non étatiques n'obtiennent les informations ou la technologie nécessaires pour utiliser les matières nucléaires à des fins malveillantes et que les systèmes de commande informatisés des installations nucléaires ne soient perturbés. Les Pays-Bas, qui exercent la présidence du Sommet sur la sécurité nucléaire, soutiennent tous les efforts déployés dans ce but.

Toujours dans le cadre du Sommet sur la sécurité nucléaire, les Pays-Bas appuient le rôle de chef de file assumé par le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord dans la mise en œuvre et l'échange de bonnes pratiques en matière de sécurité de l'information dans le secteur nucléaire. Cela implique la mise au point et le renforcement au niveau national des mesures, des dispositifs et des capacités permettant d'assurer effectivement la gestion et la sécurité de l'information dans le secteur nucléaire; le renforcement d'une culture de la sécurité au niveau national; la collaboration avec les communautés scientifique, industrielle et universitaire à l'échelon national afin de faire connaître, développer et diffuser les bonnes pratiques et de relever les normes professionnelles; le soutien, avec le concours de l'AIEA, à d'autres organisations internationales et pays partenaires

essentiels afin de favoriser la réalisation des objectifs communs. Très attachés à un modèle de gouvernance d'Internet dont personne ne soit exclu, les Pays-Bas associent le secteur privé et les organismes de recherche scientifique à ce dialogue et sont plus que disposés à partager leur expérience et leurs bonnes pratiques.

Un échange intensif de connaissances et d'informations à l'échelle internationale, entre les parties prenantes et les organisations, est essentiel pour renforcer la sécurité et la fiabilité du cyberespace et lui permettre de réaliser pleinement son potentiel, que ce soit au service du développement ou au service d'un rapprochement des sociétés du monde entier. Aussi les Pays-Bas se félicitent-ils des cyberconférences qui ont eu lieu à Londres et à Budapest, et de celle qui se tiendra à Séoul.

Enfin, les Pays-Bas considèrent que l'élaboration de normes régissant la conduite des États exige, non pas que l'on réinvente le droit international, mais que l'on veille à ce que les cadres juridiques internationaux existants soient appliqués de manière cohérente. Nous appelons donc à poursuivre le dialogue et la réflexion afin de parvenir à un consensus sur les conséquences pratiques d'une application effective des règles et du droit international existants au cyberespace.

République islamique d'Iran

[Original : anglais]
[7 juin 2013]

La République islamique d'Iran estime que les technologies utilisées dans le domaine de l'information et des communications sont, pour l'ensemble des États et l'humanité tout entière, riches de promesses. Composantes essentielles des sociétés modernes, l'informatique et les télécommunications jouent un rôle déterminant dans la richesse et la prospérité des nations. La République islamique estime que tout doit être fait, aux niveaux national et international, pour permettre à l'ensemble des nations d'utiliser le plus largement possible ces technologies et s'assurer qu'elles demeurent, dans toutes les sociétés, les principaux moteurs du développement.

Il va sans dire que pour qu'un aussi noble objectif se réalise, les États doivent pouvoir exercer une totale souveraineté dans ce domaine et, en particulier, le droit de mettre au point, d'acquérir, d'utiliser, d'importer ou d'exporter les technologies dont il est question, ainsi que les services connexes, ou d'y accéder, sans restriction ni discrimination. Il est dans l'intérêt de toutes les nations, et par conséquent de la plus haute importance, que soient garantis un constant accès à l'information ainsi que la fiabilité, l'intégrité et la sécurité de cette dernière et que soit mis en place un environnement sûr. Il est indéniable que toute mesure visant à interdire ou restreindre le transfert aux pays en développement de savoir-faire et de technologies de pointe ainsi que la fourniture de services connexes aurait un effet négatif sur le développement global de ces pays et qu'il convient, par conséquent, de se garder d'adopter ce type de mesure.

Ces technologies sont toutefois susceptibles d'être employées à des fins illicites, notamment au détriment des infrastructures et intérêts sociaux, culturels, économiques, politiques et sécuritaires des États. Alors que les sociétés dépendent de plus en plus de l'accès à l'information et des infrastructures de télécommunications, le fait que des criminels ou terroristes (qui sont parfois des États) puissent utiliser les

technologies précitées à des fins illicites met en évidence les failles actuelles et la portée des conséquences qui pourraient résulter de cette utilisation. Il est donc primordial, à l'échelle des pays, de prendre toutes les mesures appropriées, tant au niveau des infrastructures que sur les plans juridique et technique, pour renforcer la sécurité et empêcher l'utilisation de ces outils à des fins illicites.

Néanmoins, en raison de la complexité de ce domaine et de ses caractéristiques propres, à savoir l'absence de frontières, le dynamisme, l'anonymat, la vitesse et la rapidité de l'évolution technologique, mais aussi de l'interconnexion croissante des réseaux, il semble impossible d'assurer une quelconque sécurité en se contentant d'adopter des mesures au niveau national. C'est la raison pour laquelle, sachant par ailleurs que les utilisations illicites sont, dans de nombreux pays, de plus en plus fréquentes, tous les États doivent également coopérer au niveau international.

La République islamique d'Iran prend acte des efforts actuellement déployés par l'ONU et par d'autres organisations internationales dans le domaine de l'information et des communications et estime que la meilleure manière d'aborder ces questions serait de créer, au sein du systèmes des Nations Unies, un mécanisme international mettant tous les États sur un pied d'égalité. La République islamique est fermement convaincue qu'un tel mécanisme devrait avoir pour principaux objectifs d'amener les États à reconnaître l'importance d'un renforcement de la sécurité en matière d'information et de communications, à prendre la mesure de la nature, de la portée et de la gravité des menaces qui pèsent sur les technologies utilisées et à trouver moyen de les prévenir. Une telle démarche peut aboutir à l'adoption d'un programme d'action définissant les mesures devant être prises par les États Membres et pourrait prendre la forme d'un cycle de conférences internationales quinquennales qui déboucheraient sur l'élaboration d'un éventail de documents à caractère politique, allant de la déclaration au code de conduite. Son but ultime devrait néanmoins être la mise en place progressive d'un cadre juridique permettant de renforcer et de garantir, au niveau mondial, la sécurité de l'information et des communications et d'empêcher l'utilisation des technologies connexes à des fins illicites.

La République islamique d'Iran estime que ces questions doivent être abordées conformément aux principes suivants :

a) En règle générale, le droit international est applicable et doit donc s'appliquer à l'usage que font les États des technologies de l'information et des communications. Les États doivent par conséquent, dans ce domaine, se conformer aux buts et principes des Nations Unies et honorer les obligations que leur impose la Charte, notamment le devoir de régler les différends internationaux par des moyens pacifiques (par. 3 de l'Article 2), l'interdiction de recourir à la menace ou à l'emploi de la force de toute manière incompatible avec les buts des Nations Unies (par. 4 de l'Article 2) et l'interdiction de l'intervention et de l'ingérence dans les affaires intérieures des États (par. 7 de l'Article 2);

b) Rien ne doit porter atteinte à la souveraineté des États en matière d'information et de communications, s'agissant en particulier de leur droit de mettre au point, d'acquérir, d'utiliser, d'importer ou d'exporter les savoir-faire et les technologies ainsi que les services connexes, ou d'y accéder, sans aucune restriction ni discrimination. Les États doivent donc absolument s'abstenir d'adopter toutes mesures visant à interdire ou à limiter le transfert aux pays en développement de ces savoir-faire et technologies de pointe, ainsi que la fourniture des services connexes;

c) Il incombe à chaque État, et uniquement à lui, de garantir la sécurité de l'information et des communications au niveau national. Toutefois, en raison de la dimension planétaire des technologies de l'information et des communications, les États devraient être encouragés à coopérer afin de prévenir les menaces découlant de leur utilisation malveillante;

d) Le droit à la liberté d'expression doit être pleinement respecté, mais l'exercice de ce droit ne doit en aucun cas être contraire aux buts et principes des Nations Unies, aux législations nationales et aux principes relatifs à la sûreté de l'État, à l'ordre public, à la santé publique, à l'ordre moral et à la bienséance;

e) Les États sont responsables des actions internationalement illicites qu'ils commettent en utilisant les technologies de l'information et des communications et qui peuvent leur être manifestement imputées;

f) L'instauration, dans l'intérêt de tous les pays, d'un climat de sécurité en matière d'information et de communications, devrait être un principe fondamental. Les États doivent par conséquent s'abstenir, en toutes circonstances, d'utiliser les technologies de l'information et des communications à des fins hostiles, contraignantes ou illicites, notamment en mettant au point ou en utilisant des armes informatiques dans le but de fragiliser ou de déstabiliser les systèmes politiques, économiques ou sociaux d'autres États ou de porter atteinte à leurs valeurs culturelles, éthiques ou religieuses, ainsi que de diffuser des informations au-delà de leurs frontières en violation du droit international, en particulier de la Constitution et des règlements de l'Union internationale des télécommunications, ou de la législation des pays visés;

g) Les États doivent mener, aux niveaux national et international, une action de sensibilisation à la nécessité de protéger et d'améliorer la sécurité de l'information et des communications grâce à une utilisation responsable des technologies appropriées, en vue de favoriser l'émergence d'une culture internationale commune de la sécurité de l'information et des communications.

Turquie

[Original : anglais]
[10 juin 2013]

Observations générales sur la sécurité de l'information

À l'heure du village mondial et du recours de plus en plus généralisé aux technologies de l'information, assurer la sécurité de l'information est devenu une nécessité. La sécurité de l'information et la cybersécurité sont des questions qui doivent être gérées en collaboration avec toutes les parties concernées. Le Conseil des ministres turc a établi, dans sa décision sur la mise en œuvre, la gestion et la coordination des études nationales sur la cybersécurité, publiée au *Journal officiel* n° 28447 du 20 octobre 2012, le Conseil de la cybersécurité, mécanisme central de coordination des parties prenantes et de suivi des études pertinentes.

Au cours de sa première réunion, tenue le 20 décembre 2012, le Conseil a approuvé la stratégie nationale de cybersécurité, assortie d'un plan d'action pour 2013-2014.

Les objectifs de la stratégie et du plan d'action sont les suivants :

- Créer une infrastructure permettant aux organisations gouvernementales d'accéder aux services, mécanismes et données mis à disposition grâce aux technologies de l'information;
- Garantir la sécurité des systèmes d'information utilisés dans les infrastructures essentielles administrées par le gouvernement ou le secteur privé;
- Définir des mesures stratégiques de cybersécurité afin de réduire le plus possible les effets des cyberattaques et les délais de reprise après une attaque;
- Établir une infrastructure facilitant le travail d'enquête mené par les autorités judiciaires et les autorités de police en matière de cybercriminalité.

Les principaux domaines sur lesquels porte le plan d'action sont les suivants :

1. Réglementation;
2. Études visant à faciliter les procédures judiciaires;
3. Établissement d'une équipe nationale d'intervention informatique d'urgence;
4. Renforcement de l'infrastructure nationale de cybersécurité;
5. Formation et sensibilisation des ressources humaines à la cybersécurité;
6. Développement de technologies nationales en faveur de la cybersécurité;
7. Élargissement de la portée des mécanismes nationaux de cybersécurité.

Le plan d'action comporte 29 mesures portant sur ces grands domaines.

Efforts entrepris au niveau national pour renforcer la sécurité de l'information et promouvoir la coopération internationale dans ce domaine

L'Agence des technologies de l'information et des communications, organe national de contrôle créé par la loi nº 5809 sur les communications électroniques, s'efforce, dans le cadre de ses diverses activités, de contribuer à l'action menée pour répondre aux exigences nationales et internationales en matière de sécurité de l'information.

Les activités qu'elle mène dans le domaine de la cybersécurité sont exposées ci-dessous.

1. Réglementation et inspections

Plusieurs conditions concernant les opérateurs agréés sont définies dans l'arrêté sur la sécurité des communications électroniques et le communiqué y relatif qui se fonde sur cet arrêté. Les études pertinentes visent à améliorer le niveau de cybersécurité nationale directement dans les activités des opérateurs et à contribuer implicitement à la cybersécurité internationale.

L'Agence a également adopté des règles concernant la signature électronique et les lettres recommandées électroniques dans le cadre de la loi sur la signature électronique (nº 5070) et de la loi sur le commerce (nº 6112), qui contribuent toutes

deux aux efforts déployés pour promouvoir la sécurité et la fiabilité des échanges de documents et de courriels.

2. Exercices de cybersécurité

L'Agence des technologies de l'information et des communications organise des exercices de cybersécurité afin de renforcer les capacités techniques et administratives, de sensibiliser l'opinion publique et de faciliter la coopération internationale.

2.1 Exercice national de cybersécurité de 2011

Ont participé à l'exercice national de cybersécurité de 2011, qui s'est tenu du 25 au 28 janvier 2011, 41 organisations publiques, privées et non gouvernementales représentant les secteurs de la finance, des technologies de l'information et des communications, de l'éducation, de la défense et de la santé, ainsi que les autorités judiciaires et de police et divers ministères. Six d'entre elles étaient dotées du statut d'observateur.

2.2 Exercice bouclier cybernétique de 2012

Cet exercice, coordonné par l'Agence des technologies de l'information et des communications, a eu lieu en mai 2012. Douze fournisseurs d'accès à Internet travaillant dans le secteur des communications électroniques y ont participé. Ces participants détenaient la plus large part de marché dans le secteur ou fournissaient des services de téléphonie mobile de troisième génération. L'exercice a consisté pour l'essentiel à exposer les participants à des dénis de service distribué et à évaluer l'efficacité des mesures de sécurité prises pour y remédier.

2.3 Exercice national de cybersécurité de 2013

L'exercice national de cybersécurité de 2013, organisé par l'Agence des technologies de l'information et des communications et le Conseil turc de la recherche scientifique et technique sous les auspices du Ministère des transports, des affaires maritimes et des communications, a eu lieu du 24 décembre 2012 au 11 janvier 2013. Soixante et une organisations publiques, privées et non gouvernementales y ont pris part, mais la majorité des participants étaient des entités publiques. En outre, le Président du partenariat UIT-IMPACT [Union internationale des télécommunications-Partenariat multilatéral international contre les cybermenaces (IMPACT)] et un membre du Conseil d'administration du Forum des équipes de veille et de réponse aux incidents de sécurité informatique qui sont des mécanismes de coopération internationale en matière de cybersécurité, ont prononcé une déclaration lors de la clôture de l'exercice.

3. Projet concernant la prévention des cybermenaces

Le projet concernant la prévention des cybermenaces (Siber Tehditleri Önleme Projesi – STOP) prévoit l'élaboration de mécanismes nécessaires à l'établissement d'un serveur piège permettant de détecter les cybermenaces, la mise en place et le perfectionnement d'un système d'alerte en cas de cyberattaque et la production de métadonnées sur les cybermenaces. Les activités prévues par le projet sont menées à bien dans le respect des délais fixés dans le plan d'action national en matière de cybersécurité à court terme. Dans le cadre de la coopération internationale inhérente

au projet, l'Agence des technologies de l'information et des communications est devenue membre du partenariat UIT-IMPACT, qui relève de l'UIT.

4. Projet concernant la prévention des pourriels

Le projet, coordonné par l'Agence des technologies de l'information et des communications avec le concours de fournisseurs d'accès à Internet et de fournisseurs de services d'hébergement, a été mené en 2009. Son objectif était de prévenir les pourriels, qui menacent la sécurité des réseaux et mobilisent leurs ressources. À l'issue du projet, le nombre de fournisseurs d'accès à Internet propageant des pourriels a été réduit de 99 %, ainsi qu'il ressort des rapports établis par plusieurs entreprises mondiales de cybersécurité.

5. Établissement d'un point d'échange Internet dans le pays

La pratique de routage des fournisseurs d'accès à Internet qui consiste à faire circuler inutilement le trafic Internet d'un point d'extrémité à un autre à partir d'un point éloigné entraîne une diminution de la qualité du service en raison de l'allongement du temps de transmission et de l'augmentation des problèmes de sécurité.

C'est pourquoi, en établissant un point d'échange Internet et en permettant aux opérateurs d'échanger leur trafic dans des conditions plus attrayantes, ces pratiques de routage non désirées et les problèmes de sécurité qu'elles entraînent peuvent être considérablement réduits. L'Agence des technologies de l'information et des communications mène donc différentes activités avec les parties concernées (les fournisseurs d'accès à Internet dans le pays et les fournisseurs internationaux de contenu) axées sur la création, dans le pays, d'un point d'échange Internet efficace.

Mesures de renforcement de la sécurité de l'information au niveau mondial

Établissement d'une équipe nationale d'intervention informatique d'urgence

À l'heure actuelle, il faut créer une organisation pour répondre aux cyberincidents, chargée, au niveau national, de détecter les cybermenaces émergentes, de prendre les mesures qui s'imposent pour réduire ou éliminer les effets des cyberincidents potentiels et d'échanger des informations. Dans cette optique, le Ministère des transports, des affaires maritimes et des communications a chargé, en février 2013, la Présidence des communications d'établir et de diriger l'équipe nationale turque d'intervention informatique d'urgence, qui sera opérationnelle 7 jours sur 7, 24 heures sur 24. Des mesures ont été prises en ce sens. L'équipe, qui a commencé ses activités en mai 2013, travaillera en étroite collaboration avec ses pairs d'autres pays et d'organisations internationales.

Compte tenu du développement rapide et de la prolifération des systèmes informatiques et des télécommunications, les menaces qui pèsent sur la sécurité de l'information vont au-delà des frontières nationales. Il est par conséquent essentiel que les organisations internationales et les gouvernements promeuvent les activités de coopération dans le domaine de la sécurité de l'information et en assure concrètement la mise en œuvre dès que possible.