Nations Unies A/72/315

Assemblée générale

Distr. générale
11 août 2017
Français
Original : anglais/arabe/espagnol/
français/russe

Soixante-douzième session
Point 95 de l'ordre du jour provisoire*

Progrès de l'informatique et des télécommunications et sécurité internationale

Rapport du Secrétaire général

Table des matières

* A/72/15.

17-13876 (F) 220917 250917

I. Introduction

1. Le 5 décembre 2016, l'Assemblée générale a adopté la résolution 71/28, intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale ». Au paragraphe 3 de cette résolution, l'Assemblée générale a invité 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 l'informatique et des télécommunications dans le contexte de la sécurité internationale (A/70/174), leurs vues et observations sur les questions suivantes :

a) L'ensemble des questions qui se posent en matière de sécurité informatique;

b) Les actions engagées au niveau national pour renforcer la sécurité informatique et promouvoir la coopération internationale dans ce domaine;

c) Le contenu des principes visés au paragraphe 2 de la résolution;

d) Les mesures que la communauté internationale pourrait prendre pour renforcer la sécurité informatique à l'échelle mondiale.

2. Comme suite à cette demande, deux notes verbales ont été envoyées aux États Membres pour les inviter à communiquer des informations à ce sujet : la première le 16 février 2017, et la seconde le 12 juin 2017. Les réponses reçues au moment de la rédaction du présent rapport sont reproduites dans la section II ci-dessous. Les réponses reçues après le 31 juillet 2017 seront affichées, dans la langue de l'original, sur le site Web du Bureau des affaires de désarmement (https://www.un.org/disarmament/fr/).

II. Réponses reçues des gouvernements

Afghanistan

[Original : anglais]
[26 mai 2017]

En réponse au paragraphe 3 de la résolution 71/28 de l'Assemblée générale, intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », le Ministère des télécommunications et des technologies de l'information de la République islamique d'Afghanistan a transmis les informations suivantes.

Réalisations

Afin de promouvoir la sécurité informatique au niveau international et de garantir l'authenticité des transactions électroniques, le Ministère des télécommunications et des technologies de l'information a mis au point un dispositif d'infrastructure à clefs publiques. Il a également mis en place un centre d'opérations du réseau, qu'il a l'intention de raccorder au système utilisé par les États Membres à des fins de recherches et de vérification des informations circulant sur le Web et des statistiques actuelles.

Le Ministère des télécommunications et des technologies de l'information a par ailleurs soumis, pour examen, au Ministère de la justice des projets de loi qui permettraient de renforcer la sécurité des transactions électroniques et de combattre la cybercriminalité.

Le Ministère a mis au point une stratégie informatique nationale visant l'échange d'informations sécurisées, la création d'un cadre de sécurité informatique pour le lancement, dont il est lui-même chargé, du projet NIXA (National Internet Exchange Of Afghanistan), et la prévention et la détection des crimes informatiques.

Propositions

Le Ministère des télécommunications et des technologies de l'information appelle les pays développés qui sont dotés de dispositifs de lutte contre la cybercriminalité à l'aider à se munir d'outils similaires.

Pour faire face à la cybercriminalité et lutter efficacement contre ce phénomène, il est nécessaire qu'un système cohérent (qui faciliterait le partage d'informations en la matière) soit mis en place au niveau international.

La gouvernance d'Internet est un élément clef de la sécurité informatique; la promouvoir faciliterait l'échange d'informations et de données confidentielles au sujet du réseau susmentionné entre tous les départements et bureaux du Gouvernement. À cet égard, le Ministère sollicite la coopération de tous les États Membres.

Le Ministère prie également les États Membres de prêter main forte à son personnel en vue de lutter contre la cybercriminalité et d'améliorer la sécurité informatique, en lui proposant des programmes de formation professionnelle et technique.

Allemagne

[Original : anglais]
[30 mai 2017]

L'évolution des technologies de l'information et des communications (TIC) ouvre de nombreuses perspectives économiques, sociales et scientifiques, si bien qu'il est désormais essentiel, au XXI^{e} siècle, de garantir l'accès au cyberespace et de maintenir l'intégrité, l'authenticité et la confidentialité des données qu'il véhicule.

Dans un monde de plus en plus interdépendant, les États, les infrastructures essentielles, les entreprises et les particuliers sont tributaires du bon fonctionnement des TIC. Leur utilisation abusive peut avoir des conséquences qui, au-delà du cyberespace, peuvent également toucher la sphère sociale, économique ou politique. Ainsi, les attaques visant les institutions de l'État ou les mécanismes démocratiques et politiques peuvent porter atteinte à l'ordre public et à la sécurité.

Pour répondre à ces défis, l'Allemagne encourage les États à utiliser les TIC de manière à ne pas enfreindre les normes et le droit international et à favoriser le renforcement de la confiance, et ce à trois niveaux :

a) Au niveau international, l'Allemagne appuie les efforts visant à convenir de la manière dont le droit international s'applique à l'utilisation des TIC par les États et à établir des normes, règles ou principes volontaires non contraignants relatifs au comportement responsable des États, favorisant ainsi un environnement ouvert, sûr, stable, accessible et pacifique pour les TIC. Dans ce contexte, les travaux des groupes successifs d'experts gouvernementaux chargés d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale sont particulièrement importants. Les experts allemands ont participé activement aux travaux de ces groupes et l'Allemagne est résolue à promouvoir leurs recommandations. Le moment est maintenant venu d'élargir le débat pour y

associer l'ensemble des États Membres de l'ONU, en vue d'universaliser les travaux sur l'utilisation des TIC dans le contexte de la sécurité internationale. L'Allemagne est favorable à l'octroi d'un rôle de chef de file à l'ONU et au renforcement de ses capacités dans ce domaine. Parmi les questions à examiner plus avant figurent notamment le partage de l'information et la coopération internationale en matière d'établissement des responsabilités en cas de cyberattaques. Il faudrait fixer des règles claires et universelles pour combattre l'utilisation malveillante des cybercapacités ainsi que l'espionnage économique en ligne;

b) Au niveau régional, les mesures de confiance contribuent à empêcher que les incidents informatiques ne se transforment en crises politiques, voire militaires. Dans le cadre de l'Organisation pour la sécurité et la coopération en Europe (OSCE), l'Allemagne a été pendant des années très impliquée dans l'élaboration et l'application de mesures de confiance favorisant la sécurité des TIC et leur utilisation par les États. Pendant la présidence allemande de l'OSCE en 2016, les États participants sont convenus de mesures supplémentaires de ce type. Le Conseil ministériel 2016 de l'OSCE à Hambourg les a approuvées et a donné des instructions non seulement pour leur mise en œuvre, mais aussi pour la poursuite des travaux à entreprendre, qui doivent dépasser les aspects politico-militaires et favoriser la sécurité multidimensionnelle. En dehors de l'OSCE, l'Allemagne encourage également des efforts comparables dans le cadre d'organisations régionales œuvrant sur d'autres continents;

c) Au niveau bilatéral, l'Allemagne maintient le cyberdialogue, organisant régulièrement des cyberconsultations avec de nombreux partenaires. S'appuyant sur les relations de partenariat établies, l'Allemagne soutient également les efforts de renforcement des capacités des autres nations en matière de cybersécurité. Lors de l'actualisation de sa stratégie de cybersécurité en novembre 2016, le Gouvernement allemand a décidé de créer un l'Institut allemand pour la cybersécurité internationale, afin de systématiser et de démultiplier ce travail.

Les efforts de l'Allemagne en matière d'informatique et de télécommunications dans le contexte de la sécurité internationale s'inscrivent dans le cadre d'activités de promotion de la sécurité des TIC en général. Les récents dispositifs réglementaires nationaux, tels que la loi de 2015 sur la sécurité informatique et la stratégie révisée de cybersécurité de 2016, visent à améliorer la sécurité des TIC en général en Allemagne.

Arménie

[Original : anglais]
[31 mai 2017]

Ensemble des questions qui se posent en matière de sécurité informatique

Compte tenu de la place de plus en plus grande qu'occupe l'électronique dans la société arménienne, la question de la sécurité informatique gagne en pertinence, entraînant des répercussions considérables sur tous les aspects de la sécurité nationale.

L'évolution des technologies de l'information et des communications, qui pose de nouvelles menaces et de nouveaux défis de fond, se traduit par la nécessité de développer une coordination systématique et d'adopter de nouvelles approches pour veiller à leur sécurité d'utilisation. Face au recours, par différentes parties à des conflits, à des techniques de « guerre de l'information », l'Arménie attache une

grande importance à la sécurité informatique, primordiale au maintien de la paix et de la sécurité internationales.

Actions engagées au niveau national pour renforcer la sécurité informatique et promouvoir la coopération internationale dans ce domaine

L'Arménie a pris des mesures visant à préserver l'intérêt public et les intérêts de l'État dans le domaine de la sécurité informatique et modifié sa législation afin de la rendre conforme aux normes internationales. Une série de textes normatifs s'appliquant au domaine informatique ont été adoptés, notamment une stratégie de sécurité nationale et une ligne de conduite sur la sécurité informatique ainsi que des lois sur la lutte contre le terrorisme, les secrets d'État et les secrets officiels, les documents électroniques et les signatures numériques, la protection des données à caractère personnel, la liberté d'information, et les médias.

Conformément aux décisions pertinentes prises par le Gouvernement :

a) Un certain nombre de mesures concrètes ont été adoptées pour veiller à la protection des informations accessibles au public sur les sites Web des organes gouvernementaux, dont la connexion à Internet a par ailleurs été sécurisée;

b) Des normes minimales de sécurité applicables aux sites Web officiels des organes gouvernementaux ont été adoptées.

L'Arménie a adopté et appliqué une série de normes ISO relatives à la sécurité informatique. En octobre 2006, elle a ratifié la Convention du Conseil de l'Europe sur la cybercriminalité, avant d'apporter les modifications nécessaires à la législation nationale.

L'Arménie participe activement à des programmes, formations et initiatives de coopération menés dans différents cadres internationaux, tels que la Communauté d'États indépendants, l'Organisation du Traité de sécurité collective, l'Union européenne et l'Organisation du Traité de l'Atlantique Nord. En 2016, par exemple, un exercice collectif en deux étapes de lutte contre le terrorisme informatique a été réalisé par les pays membres de la Communauté d'États indépendants. Un projet d'accord de coopération entre les États membres de l'Organisation du Traité de sécurité collective visant à garantir la sécurité informatique a par ailleurs été présenté au début de 2017 en vue d'être approuvé au niveau interne par les différents départements concernés.

Contenu des principes visés au paragraphe 2 de la résolution 71/28

Dans la ligne de conduite sur la sécurité informatique adoptée par la République d'Arménie, le terme « sécurité informatique » s'entend de la protection des intérêts nationaux dans le domaine de l'informatique, et donc de celle des intérêts des individus, de la société et de l'État dans leur ensemble.

Compte tenu de l'évolution rapide des technologies de l'information et de la communication, un groupe de travail interinstitutions a été créé pour élaborer, à la fin de 2017, une nouvelle stratégie relative à la sécurité informatique et à l'information dans la République d'Arménie.

Mesures que la communauté internationale pourrait prendre pour renforcer la sécurité informatique à l'échelle mondiale

L'Arménie souligne qu'il est primordial de renforcer et d'améliorer la coopération internationale en ce qui concerne la sécurité informatique et insiste sur le rôle tenu par l'Union internationale des télécommunications.

Bélarus

[Original : russe]
[5 juin 2017]

Ensemble des questions qui se posent en matière de sécurité informatique

Actuellement, le niveau de sécurité informatique dans le monde n'est pas satisfaisant, certains tentant d'utiliser les technologies de l'information à des fins politiques.

Le Bélarus fait face à plusieurs problèmes caractéristiques en matière de sécurité informatique :

a) Un degré de protection insuffisant du segment de réseau national face aux attaques par déni de service distribué (DDoS), tant au niveau des fournisseurs généraux et internes qu'au niveau des sites d'hébergement;

b) La présence éventuelle de capacités ou de vulnérabilités non déclarées dans les outils de sécurité informatique et l'impossibilité de les détecter rapidement, qui se traduisent souvent par une baisse de l'efficacité des mesures de protection de l'information;

c) Le risque de voir des infrastructures et des installations informatiques de grande importance, telles que des systèmes d'alimentation électrique et des systèmes automatiques de gestion de la production et des transports, être la cible d'attaques destructrices.

Actions engagées au niveau national pour renforcer la sécurité informatique et promouvoir la coopération internationale dans ce domaine

Le Bélarus a notamment décidé :

a) De procéder, dans l'ensemble du système, à la mise à jour des exigences relatives à la protection technique et cryptographique des données dont la dissémination et le partage sont limités;

b) D'établir et d'appliquer des normes techniques et autres concernant la protection technique et cryptographique des informations;

c) De conclure des accords relatifs au partage d'informations avec des entreprises de premier plan dans le domaine de la sécurité informatique;

d) De collaborer en permanence avec des organisations et organismes gouvernementaux divers, en vue d'apporter une réponse rapide aux incidents ayant trait à la sécurité informatique;

e) D'entretenir son système de détection des logiciels malveillants;

f) De collaborer avec les pays membres de l'Organisation du Traité de sécurité collective par l'intermédiaire d'un centre de coordination consultatif.

Examen des stratégies internationales destinées à renforcer la sécurité des systèmes informatiques et des systèmes de télécommunication à l'échelle mondiale

Selon le Bélarus, il est primordial, en vue de remédier au problème de la sécurité informatique, d'empêcher que les technologies de l'information et des communications ne soient utilisées pour porter atteinte à la sécurité et à la stabilité du pays, ainsi qu'à la sécurité de la communauté internationale dans son ensemble.

Le Bélarus participe activement aux débats traitant de la sécurité informatique à l'échelle mondiale organisés par diverses organisations internationales, telles que l'Organisation des Nations Unies, l'Organisation du Traité de sécurité collective et l'Organisation pour la sécurité et la coopération en Europe.

Le Bélarus est favorable à l'initiative visant à adopter un instrument universel sur la sécurité informatique internationale, sous l'égide de l'Organisation des Nations Unies.

Mesures que la communauté internationale pourrait prendre pour renforcer la sécurité informatique à l'échelle mondiale

Au niveau international, il est important que les principes de non-ingérence dans les affaires intérieures d'un État souverain et de non-agression mutuelle soient progressivement mieux respectés dans le domaine de l'informatique. Pour ce faire, il importe de préserver la souveraineté en matière d'information des États Membres de l'ONU, en vue de :

a) Respecter le droit des citoyens de recevoir, de conserver et de partager des informations qui soient complètes, fiables et opportunes;

b) Parvenir à la création d'une société de l'informatique à laquelle les États Membres de l'ONU participeraient d'égal à égal;

c) Veiller à l'échange d'informations dans le cadre d'une politique intergouvernementale efficace de lutte contre la propagation des idéologies terroristes et extrémistes;

d) Garantir le bon fonctionnement à long terme des installations les plus importantes.

Mesures que la communauté internationale pourrait prendre pour renforcer la sécurité informatique à l'échelle mondiale

a) Mettre en place les mécanismes de coopération internationale prévus dans les instruments juridiques internationaux actuels et futurs;

b) Établir des liens avec les sociétés transnationales qui contrôlent une grande majorité des technologies de l'information et des communications, afin de pouvoir détecter l'origine des menaces pesant sur la sécurité informatique en vue de les contrer efficacement.

Brunéi Darussalam

[Original : anglais]
[29 juin 2017]

Le Brunéi Darussalam est conscient du fait que les progrès majeurs accomplis dans les domaines de l'informatique et des télécommunications ont fait évoluer les tendances mondiales. Il note néanmoins que ces avancées se sont accompagnées de nouvelles menaces et de nouveaux dangers, tels que le piratage informatique, la cybercriminalité et le cyberterrorisme, qui mettent en péril divers réseaux, infrastructures et services d'une importance vitale dans le monde entier. En raison de la nature transnationale et immatérielle de ces menaces, il est nécessaire que les membres de la communauté internationale agissent de concert en vue de construire un cyberespace sûr et fiable.

Au niveau national, le Brunéi Darussalam entretient, sous les auspices de son comité national de sécurité, une coopération étroite avec toute une série

d'organismes locaux de sécurité pour faire face aux menaces de cybersécurité. Son équipe d'intervention informatique d'urgence, créée en mai 2004, est devenue le point de référence en ce qui concerne la gestion des problèmes de sécurité informatique. Dans le cadre des échanges qu'elle entretient avec les équipes d'intervention informatique d'urgence d'autres pays, l'équipe reçoit des informations précieuses sur les menaces de sécurité relatives aux technologies de l'information et de la communication détectées de par le monde et partage les données pertinentes qu'elle a elle-même recueillies sur son territoire.

Le Brunéi Darussalam est résolu à œuvrer avec ses partenaires régionaux et internationaux pour faire face aux grandes cybermenaces qui pèsent sur notre monde. Dans le cadre de l'Association des nations de l'Asie du Sud-Est (ASEAN), le Brunéi Darussalam prendra part aux activités du Groupe de travail d'experts sur la cybersécurité de la Réunion des ministres de la défense de l'ASEAN (ADMM-Plus), qui réunit 18 pays et a pour objectif de promouvoir une coopération pratique et efficace dans la région, de renforcer la protection du cyberespace et de relever les défis relatifs à la cybersécurité.

Le Gouvernement du Brunéi Darussalam est conscient des menaces qui planent sur tous les domaines de l'informatique, y compris l'informatique en nuage et les systèmes de télécommunication mobiles, et a fait de cette question une de ses priorités en matière de défense et de sécurité.

Canada

[Original : anglais]
[17 juillet 2017]

Concernant le cyberespace, le Canada estime que :

a) Un cyberespace libre, ouvert et sécurisé est essentiel à la sécurité, à la prospérité et au respect des droits de l'homme;

b) Le droit international actuel s'applique à l'utilisation par les États des technologies de l'information et des communications;

c) Promouvoir des normes applicables en temps de paix contribue à créer un environnement placé sous le signe de la responsabilité des États;

d) Les mesures de confiance sont un moyen avéré de réduire le risque de conflits armés.

Au niveau national, le Gouvernement canadien a récemment fini de réviser la stratégie de cybersécurité qu'il avait adoptée en 2010 en vue de renforcer la sécurité de ses systèmes informatiques et de protéger les utilisateurs d'Internet. Cette nouvelle version de la stratégie, qui devrait être adoptée à la fin de 2017, prévoit de nouveaux investissements et contient des directives générales devant permettre de mieux exploiter les cybercapacités à l'appui des opérations militaires. L'utilisation des cybercapacités actives par les forces armées canadiennes sera soumise aux mêmes critères que celle des autres outils militaires, y compris en ce qui concerne le respect du droit national et international et les règles d'engagement et de comportement.

Au niveau international, le Canada mène diverses activités :

a) Il continue de promouvoir la mise au point de normes applicables en temps de paix relatives au comportement des États dans le cyberespace, notamment les textes issus des réunions tenues en 2012-2013 et en 2014-2015 par les Groupes

d'experts gouvernementaux chargés d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale;

b) Il a ratifié, en juillet 2015, la Convention du Conseil de l'Europe sur la cybercriminalité (signée à Budapest) et il encourage les autres pays à y adhérer ou à s'en inspirer pour mettre en place leurs propres législations en la matière;

c) Depuis 2007, il apporte une contribution, qui s'élève désormais à 11 millions de dollars, à des projets de renforcement des capacités en matière de cybersécurité;

d) Il collabore avec les États-Unis d'Amérique pour mettre en œuvre le plan d'action Canada-États-Unis sur la cybersécurité, qui vise à renforcer la résilience de la cyberinfrastructure du pays;

e) Il participe à l'élaboration de mesures de confiance dans diversesinstances, dont l'Organisation pour la sécurité et la coopération en Europe et le Forum régional de l'Association des nations de l'Asie du Sud-Est;

f) Il appuie les efforts déployés par l'Organisation du Traité de l'Atlantique Nord pour renforcer la cybersécurité de l'alliance et celle de différents alliés.

Cuba

[Original : espagnol]
[5 avril 2017]

Ainsi que l'Assemblée générale l'a souligné dans sa résolution 71/28, les innovations scientifiques et techniques peuvent se prêter à des applications civiles aussi bien que militaires, si bien qu'il faut veiller à ce qu'elles ne compromettent pas la sécurité internationale.

Il est nécessaire d'encourager, au niveau multilatéral, l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information et de promouvoir des stratégies susceptibles de les prévenir et d'y parer.

La coopération entre tous les États est le seul moyen d'éviter que le cyberespace ne devienne le théâtre d'opérations militaires.

Cuba soutient les travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, créé par la résolution 58/32, qui compte un expert cubain.

Nous estimons nécessaire d'élaborer un cadre international juridiquement contraignant, applicable aux technologies de l'information et des communications, qui complète le droit international en vigueur.

Lorsqu'ils sont conçus ou utilisés dans le but de porter atteinte à l'infrastructure d'un État, les systèmes informatiques et de télématiques peuvent devenir des armes. Tous les États doivent respecter les normes internationales en vigueur en la matière. L'accès aux systèmes informatiques et télématiques d'un autre État ne peut se faire que dans le respect des accords de coopération internationaux et avec le consentement de l'État concerné. Les modalités et la nature des échanges doivent être conformes à la législation de cet État.

L'usage hostile des télécommunications, dans le but déclaré ou inavoué de perturber l'ordre juridique et politique des États, constitue une atteinte aux normes reconnues sur le plan international en la matière. Cette utilisation illégale et irresponsable est susceptible de générer des tensions, de peser sur la paix et la

sécurité internationales, et de menacer l'intégrité de l'infrastructure des États, compromettant ainsi leur sécurité tant en matière civile que militaire.

Cuba réitère la crainte que lui inspire l'infiltration illégale d'individus, à des fins d'agression, d'organisations ou d'États dans les systèmes informatiques et télématiques d'autres pays, en raison des conflits internationaux qu'elle risque de déclencher.

L'espace radiophonique cubain est régulièrement violé par des personnes ou entités étrangères qui y diffusent des émissions de radio et de télévision illégales, notamment des programmes visant spécialement à inciter au renversement de l'ordre constitutionnel établi par le peuple cubain. En 2016, 1 875 heures d'émissions hebdomadaires anticubaines ont été diffusées depuis le territoire des États-Unis d'Amérique, sur 25 fréquences. La diffusion continue, à Cuba, d'émissions radiophoniques et télévisuelles depuis les États-Unis est contraire aux buts et principes de la Charte des Nations Unies, du droit international et des règles de l'Union internationale des télécommunications.

Cuba demande instamment, une fois de plus, que cessent ces politiques agressives qui nuisent à la souveraineté de Cuba et empêchent l'établissement entre les États de rapports fondés sur le respect et la coopération.

Cuba attend également que soit levé le blocus économique, commercial et financier, qui est à l'origine de graves souffrances pour le peuple cubain et a des conséquences négatives dans le domaine de l'informatique et des communications, entre autres domaines de la vie quotidienne du peuple cubain.

Lors du deuxième sommet de la Communauté des États d'Amérique latine et des Caraïbes (CELAC), tenu à la Havane en janvier 2014, les chefs d'État et de gouvernement d'Amérique latine et des Caraïbes ont déclaré cette région zone de paix, afin de permettre aux États, malgré les différences qui les séparent du point de vue de leurs systèmes politiques, économiques et sociaux ou de leurs niveaux de développement, d'instaurer entre eux des relations d'amitié et de coopération, en vue de favoriser la tolérance et la coexistence pacifique, dans un esprit de bon voisinage.

Les participants au cinquième Sommet de la CELAC, tenu à Punta Cana (République dominicaine) en janvier 2016, ont à nouveau mis en avant l'importance des technologies de l'information et des communications, notamment l'Internet, pour la paix, le bien-être, le développement, les connaissances, l'inclusion sociale et la croissance économique.

Cuba réaffirme que la coopération internationale est indispensable face à la menace que constitue le détournement de ces technologies, soulignant en outre le rôle majeur de l'Union internationale des télécommunications dans les débats intergouvernementaux sur les questions de cybersécurité.

El Salvador

[Original : espagnol]
[24 mai 2017]

S'agissant des obligations envers l'Organisation des Nations Unies, El Salvador souligne qu'en ce qui concerne la résolution 71/28 de l'Assemblée générale, intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », ses forces armées se sont dotées, en 2016, d'un système de cryptage des documents institutionnels pour renforcer la sécurité de l'information, lequel est en cours de déploiement.

Équateur

[Original : espagnol]
[28 juillet 2017]

L'Équateur estime que la sécurité en matière de relations internationales doit s'appuyer sur la confiance et le respect entre les États. Les affaires d'espionnage massif et indiscriminé des communications de tous les citoyens de la planète qui sont constamment révélées, de même que l'utilisation des technologies de l'information et des communications contraire au droit international, portent atteinte aux principes du respect de la souveraineté et de la non-ingérence dans les affaires intérieures des États et déstabilisent gravement les relations entre les États, compromettant ainsi la sécurité internationale. Ces activités d'espionnage portent également atteinte à divers droits de l'homme.

C'est pourquoi, l'Équateur appuie les efforts visant à poursuivre l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information, des mesures collectives permettant d'y parer ainsi que de l'applicabilité du droit international à l'utilisation des technologies de l'information et des communications par les États, et encourage l'étude des normes, règles et principes de comportement responsable des États en la matière.

Estonie

[Original : anglais]
[31 mai 2016]

L'Estonie est consciente que la question de la cybersécurité occupe désormais une place majeure dans le contexte plus large de la sécurité internationale, augmentant d'autant l'importance du rôle et de la contribution de l'Organisation des Nations Unies.

La cybersécurité est une des priorités majeures du Gouvernement estonien. La stratégie nationale de cybersécurité (2014-2017) est le principal document d'orientation sur cette question. Le Conseil de cybersécurité du Comité national de sécurité encourage la coopération interinstitutions en matière stratégique et supervise la réalisation des objectifs de la stratégie de cybersécurité. Au 30 mai 2017, le Centre d'excellence pour la cyberdéfense en coopération de l'Organisation du Traité de l'Atlantique Nord, fondé à Tallinn, comptait 20 États Membres contributeurs.

L'Estonie estime que, face à la généralisation de l'utilisation des services numériques, il est indispensable d'accroître la cybersécurité. Les dimensions socioéconomique et politico-militaire de la cybersécurité sont interdépendantes. Il est primordial que les pays s'abstiennent d'attaquer des infrastructures nationales essentielles. L'Estonie préconise également l'adoption d'un comportement responsable envers l'infrastructure mondiale de télécommunications qui soit de nature à promouvoir l'accès à l'information ainsi que la confiance à l'égard des technologies de l'information et des communications (TIC) Elle considère qu'il incombe à chaque pays d'élaborer et d'appliquer des législations nationales permettant de contrôler l'utilisation malveillante des TIC par des acteurs non étatiques et de rechercher des moyens de mieux formuler, diffuser et promouvoir les cyberpolitiques et discours relatifs au comportement responsable des États.

Pour la quatrième fois consécutive, l'Estonie est membre du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Ce forum très

productif pourrait se révéler efficace non seulement pour étudier les cybermenaces et les parades possibles mais également pour comprendre comment les différents pays appliquent le droit, les normes, les règles et les principes internationaux en vigueur. L'Estonie est d'avis que le Groupe devrait continuer à promouvoir le dialogue entre les États Membres, facilitant ainsi l'échange d'informations et de pratiques optimales. Il devrait également examiner les mesures et mécanismes concrets de coopération pour promouvoir le renforcement des capacités des États Membres, en vue de doter les États membres des compétences et des moyens nécessaires pour résoudre tous les problèmes liés au cyberespace.

Il est primordial de poursuivre les progrès réalisés lors des réunions du Groupe d'experts gouvernementaux tenues entre 2014 et 2015, en continuant de promouvoir des normes de comportement des États axés sur l'ouverture, la responsabilité et d'autres valeurs démocratiques dans le cyberespace. L'Estonie espère que le Groupe présentera un autre rapport de consensus en juin 2017.

Finlande

[Original : anglais]
[21 juillet 2017]

La Finlande se réjouit de l'occasion qui lui est donnée de fournir des informations relatives à la mise en œuvre de la résolution 71/28 de l'Assemblée générale.

Les efforts déployés au niveau national sont, entre autres, les suivants :

a) La Stratégie nationale de cybersécurité (2013) et son programme actualisé de mise en œuvre (2017), qui définissent les lignes directrices et les principales mesures à prendre pour renforcer la cybersécurité et la résilience;

b) La création d'un Centre national de la cybersécurité et d'un Centre pour la prévention de la cybercriminalité ainsi que la nomination, au sein du Ministère des affaires étrangères, d'un ambassadeur pour les affaires de cybercriminalité, et l'adoption, en 2016, de la Stratégie nationale de sécurité informatique;

c) La participation active à la coopération sur le cyberespace dans le cadre de l'Union européenne;

d) Le soutien à divers types de technologies de l'information et des communications dans le cadre de projets de développement et de renforcement des capacités en lien avec le cyberespace. Membre fondateur du Forum mondial sur la cybercompétence et en 2016, la Finlande a rejoint le Fonds d'affectation spéciale de la Banque mondiale pour le partenariat pour le développement numérique, et soutient l'application d'un modèle multipartite à la gouvernance d'Internet. Elle a participé activement au Sommet mondial sur la société de l'information et à son processus de suivi, notamment en contribuant aux travaux du Forum sur la gouvernance d'Internet et à leur financement. Le huitième Forum finlandais sur le cyberespace a eu lieu à Helsinki en avril 2017;

e) La participation active au dialogue international sur les questions liées à l'Internet dans le cadre d'instances multilatérales ou régionales et à titre bilatéral, notamment au sein de l'Organisation pour la sécurité et la coopération en Europe (OSCE), où la Finlande participe au renforcement de la confiance, de la sécurité et de la stabilité dans le cyberespace et met en œuvre les mesures propres à accroître la confiance dans le cyberespace;

f) L'approbation, en 2015, du rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et la contribution active à ses travaux. La Finlande a pris part aux discussions sur le droit international dans le cyberespace, notamment lors des consultations sur la version 2.0 du Manuel de Tallinn et des ateliers de l'Institut des Nations Unies pour la recherche sur le désarmement;

g) L'adhésion à la Freedom Online Coalition en 2012 et sa contribution au Digital Defenders Partnership ainsi que l'organisation, à Helsinki en 2016, de la Conférence de la Journée mondiale de la liberté de la presse;

h) La Finlande est partie à la Convention du Conseil de l'Europe sur la cybercriminalité. Le nouveau Plan stratégique de la police (2015) porte sur les ressources nécessaires à la prévention de la cybercriminalité et au développement du savoir-faire en matière de cybersécurité. Un plan global de prévention de la cybercriminalité a d'autre part été adopté.

Les domaines prioritaires suivants appellent davantage d'efforts de la part de la communauté internationale :

a) Les travaux de l'actuel Groupe d'experts gouvernementaux, auxquels la Finlande attache une grande importance et est disposée à contribuer, notamment la définition des normes de comportement responsable des États dans le cyberespace, en mettant tout particulièrement l'accent sur les activités en temps de paix;

b) L'adoption et la mise en œuvre de mesures de confiance à l'échelon régional, dans le cadre de l'OSCE;

c) La poursuite du renforcement des cybercapacités en vue d'améliorer la résilience et la sécurité dans le cyberespace;

d) La poursuite de la promotion du dialogue multipartite et le renforcement des partenariats public-privé aux niveaux national et international.

Grèce

[Original : anglais]
[26 mai 2017]

Dans le cadre du Conseil de l'Europe, la Grèce a ratifié, en vertu de la loi n° 4411/2016 (Journal officiel A´ 142, 3 août 2016), la Convention du Conseil de l'Europe sur la cybercriminalité (Budapest, 23/11/2001) et son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (Strasbourg, 28 janvier 2003).

Il convient de noter que la législation nationale inclut déjà un dispositif d'intégration de la directive de l'Union européenne sur la sécurité des réseaux et systèmes informatiques. Cette directive, capitale pour le renforcement de la résilience face aux cyberattaques au niveau national, fixe un certain nombre d'obligations pertinentes pour tous les États Membres de l'Union européenne et prévoit aussi l'adoption d'une stratégie nationale sur la sécurité des réseaux et systèmes informatiques.

Le Ministère de la défense informe que la Grèce entend déployer toutes ses capacités en matière de cybersécurité afin de défendre ses infrastructures et réseaux nationaux contre les cybermenaces et cyberattaques criminelles les plus récentes. Ce travail suppose que les plus hautes sphères stratégiques des organisations chargées de la défense nationale se penchent sur la question de la cyberdéfense, en intégrant

davantage la cyberdéfense dans les opérations et en veillant à ce qu'elle couvre les réseaux qui ne sont pas encore déployés. Les efforts suivants ont été faits au niveau national pour renforcer la sécurité informatique et promouvoir la coopération internationale :

a) Un cadre stratégique national de cyberdéfense est actuellement en cours d'élaboration, tandis que la stratégie nationale de cybersécurité qui réglemente le cadre général de cybersécurité et définit les mesures nécessaires pour assurer la conformité aux exigences minimales de cybersécurité acquiert force de loi;

b) La cyberdéfense fait déjà partie des plans d'opérations de défense nationale et le système national d'alerte d'urgence a été intégré dans la plupart des documents d'orientation relatifs aux systèmes informatiques et dans tous les grands exercices nationaux. La cybersécurité a été incluse dans les plans d'opérations en cas de crise de tous les organismes publics;

c) La Grèce a développé ses capacités d'intervention d'urgence dans le cadre du Centre de cyberdéfense militaire et ne cesse de les renforcer. Des équipes d'intervention rapide peuvent se déployer dans des délais courts afin de faire face aux cyberincidents qui s'en prennent aux réseaux publics ou militaires. Les documents de sécurité informatique comprennent des instructions en cas de faille ou de cyberattaque;

d) Un centre d'opérations de cybersécurité pour tous les réseaux nationaux de défense militaire est en cours de construction, tandis qu'au niveau national, il existe quatre équipes d'intervention informatique d'urgence responsables des secteurs public et privé.

Afin d'accroître la sécurité informatique, la communauté internationale pourrait :

a) Renforcer les capacités d'intervention, de surveillance du réseau et de défense mobilisables en cas de cybermenaces grâce à des centres d'opérations nationaux chargés de la cybersécurité pleinement opérationnels;

b) Procéder à une intégration complète de la cyberdéfense dans les opérations;

c) Élaborer des stratégies nationales de cybersécurité et de cyberdéfense;

d) Améliorer les connaissances en cybersécurité du personnel employé dans le secteur de la cyberdéfense et le renforcement des capacités techniques existantes;

e) Assurer la formation continue du personnel employé dans les organisations de cyberdéfense;

f) Harmoniser les législations nationales avec les lois et directives mondiales en matière de cybersécurité.

La police grecque informe que, conformément à l'article 30 du décret présidentiel n° 178/2014, la Division de la cybercriminalité a pour mission, entre autres, de prévenir les crimes utilisant l'Internet ou d'autres moyens de communication, d'enquêter, le cas échéant, sur de tels crimes, et d'en poursuivre les auteurs. Il s'agit d'un service central autonome dépendant directement du chef de la police grecque.

Une des unités de la Division est responsable de la sécurité des communications électroniques et téléphoniques ainsi que de la protection des logiciels et du droit d'auteur. Plus précisément, le Groupe enquête sur les cas d'infiltration illégale des systèmes informatiques ainsi que de vol, de destruction ou

de trafic de logiciels, de données numériques et d'œuvres audiovisuelles dans tout le pays.

La Division de la cybercriminalité coopère étroitement avec l'Autorité nationale de lutte contre les attaques électroniques, qui fait partie du Service national de renseignement. L'Autorité est chargée de contribuer à la prévention des attaques visant des réseaux de communication électroniques, des installations de stockage de données et des systèmes informatiques et télématiques, et de contribuer activement ou passivement à les contrer. Elle est en outre chargée de traiter les données et de faire rapport aux autorités compétentes.

Japon

[Original : anglais]
[27 juillet 2017]

Le Japon estime que le cyberespace doit être un espace où la liberté est assurée sans restriction inutile et où tous les acteurs souhaitant y accéder ne doivent pas se voir refuser cet accès ou en être exclus sans motif légitime. Les efforts du Japon obéissent aux cinq principes que sont la libre circulation de l'information, l'état de droit, l'ouverture, l'autonomie et l'approche multipartite.

Conformément à sa stratégie de cybersécurité publiée en septembre 2015, le Japon travaille à renforcer la sécurité informatique.

Les travaux du Japon s'appuient sur les trois piliers suivants : la promotion de la primauté du droit dans le cyberespace, les mesures de confiance et le renforcement des capacités.

En ce qui concerne la promotion de la primauté du droit, le Japon contribue activement au débat international en faveur d'une conception commune selon laquelle le droit international actuel s'applique au cyberespace et à l'élaboration de normes non contraignantes et volontaires. Celles-ci posent les jalons des efforts visant à garantir la stabilité et la prévisibilité de la communauté internationale. Vu le caractère unique des technologies de l'information et des communications, il convient de préciser la manière dont les règles et principes individuels seront appliqués.

Il importe d'assurer la transparence et le partage des informations pour promouvoir les mesures de confiance; toutefois, l'ampleur des mesures prises varie d'un État à l'autre, car chaque État est en droit de décider de celles qu'il souhaite appliquer. Le Japon participe à l'instauration de la confiance par le dialogue bilatéral et dans des cadres multilatéraux, tels que le Forum régional de l'Association des nations de l'Asie du Sud-Est. Il est nécessaire d'examiner les moyens à mettre en œuvre pour une coopération concrète.

S'agissant du renforcement des capacités, le Japon a encouragé l'élaboration de lois, de réglementations et de politiques relatives à la cybersécurité, et veille à rendre les organismes gouvernementaux et les opérateurs de TIC à même d'appliquer des mesures de lutte contre la cybercriminalité, de mettre en valeur les ressources humaines pour disposer d'experts en cybersécurité et de favoriser la recherche et le développement de technologies en matière de cybersécurité. Le Japon continuera de contribuer activement au renforcement des capacités en s'appuyant sur l'expérience et les connaissances accumulées dans ce domaine.

Jordanie

[Original : arabe]
[23 mars 2017]

L'informatique et les communications sont devenues essentielles dans notre vie quotidienne. Elles favorisent le développement et le progrès au niveau local dans tous les domaines, notamment social, culturel et économique et ont de multiples conséquences sur l'individu dans la société, favorisant son ouverture sur le monde à bien des égards.

L'informatique et les communications ont connu une progression fulgurante, ce qui les rend vulnérables aux risques existants, d'où la nécessité de les combattre au moyen de la technologie et du droit et de trouver des solutions pratiques et efficaces permettant de lutter contre ces dangers et d'éviter les lourdes pertes qu'ils peuvent occasionner.

Les forces armées jordaniennes contribuent activement et résolument à la promotion de la sécurité et de la paix aux niveaux national, régional et mondial en développant et en utilisant la technologie afin de garantir la sécurité de l'information et des télécommunications, comme en témoignent les initiatives ci-après :

a) Mise à jour de tous les systèmes de communication et de transmission de l'information par l'installation de réseaux protégés utilisant la technologie IP cryptée dans tout le Royaume, y compris aux frontières, pour renforcer la sécurité nationale et régionale;

b) Coopération avec la communauté internationale en vue du maintien de la sécurité internationale au moyen d'un recours à des systèmes de communication compatibles avec ceux utilisés par l'Organisation du Traité de l'Atlantique Nord et l'armée américaine, et conformes aux normes internationales de cryptage de haut niveau (type 1);

c) Renforcement des capacités techniques par l'acquisition de systèmes de communication ne reposant pas sur l'infrastructure pour sécuriser les zones de conflit, les camps de réfugiés et les zones reculées. Ces technologies permettent également de renforcer la sécurité nationale et d'apporter un soutien aux forces armées jordaniennes-armée arabe dans le cadre des opérations de maintien de la paix dans des zones de conflit dans le monde;

d) Formation de l'ensemble des usagers et des parties concernées à la pérennité et à la protection des systèmes de communication, sans s'en remettre aux prestataires, pour en rehausser la fiabilité et pouvoir ainsi les utiliser en tout temps;

e) Adoption des normes les plus strictes en matière de commande et de contrôle des systèmes utilisés par les armées pour resserrer la coordination et la coopération, de sorte à renforcer la sécurité nationale, régionale et internationale;

f) Participation active aux conférences internationales et application des décisions qui en découlent pour assurer une complémentarité plus grande entre les armées amies, éviter les perturbations et les interférences entre les systèmes de communication utilisés par les pays voisins et les pays de la région et coordonner les mesures de contrôle et de surveillance des frontières internationales.

Il faut veiller en permanence à ce que les citoyens aient conscience des risques liés aux cybermenaces, de la manière dont la cybersécurité permet de les réduire et du rôle que jouent les systèmes de communication à cet égard. Les utilisateurs doivent en outre avoir une meilleure connaissance des risques en matière de sécurité

liés à la manipulation de l'information, quelle qu'elle soit, sans que cela n'entrave leur recours aux technologies et les bénéfices qu'ils en tirent.

Les mesures ci-après ont été adoptées à l'échelle nationale pour protéger les réseaux informatiques essentiels :

a) Cryptage de tous les réseaux et systèmes de communication vocale, de données et vidéo;

b) Utilisation de réseaux fermés (intranet);

c) Liaison avec les autres organismes de sécurité au moyen de dispositifs périphériques indépendants;

d) Application de mesures destinées à garantir la sécurité de l'information et des communications et du principe du besoin d'en connaître et vérification systématique des autorisations d'accès et de l'identité des utilisateurs;

e) Utilisation de réseaux virtuels par lesquels les utilisateurs interagissent avec un écran connecté au système grâce à des autorisations d'accès. L'accès ou la connexion ne peut pas se faire par d'autres moyens, comme l'utilisation d'une clef USB;

f) Adoption et promulgation d'une série de lois relatives à la sécurité de l'information, à savoir :

1. Adoption d'une loi sur la cybercriminalité;

2. Adoption d'une loi sur les transactions électroniques;

3. Ébauche d'une stratégie nationale relative à la sécurité et à la protection de l'information;

4. Ébauche de mesures nationales visant à garantir la sécurité et la protection de l'information;

5. Adoption par le Conseil des ministres en 2012 de la Stratégie nationale en matière de sécurité de l'information et de cyberprotection.

La Jordanie propose les initiatives suivantes au plan mondial :

a) Classer les réseaux d'information et de communication par ordre d'importance;

b) Mettre en œuvre des mesures visant à garantir la protection et la sécurité des données;

c) Appliquer le principe du besoin d'en savoir;

d) Utiliser les techniques de cryptage et de saut de fréquence;

e) Vérifier et classer les utilisateurs et les autorisations d'accès aux sites et aux réseaux;

f) Connecter les différents réseaux par des périphériques indépendants;

g) Recourir à un intranet privé dans certains réseaux et éviter autant que possible d'utiliser la toile mondiale;

h) Renforcer l'intranet de l'Organisation des Nations Unies, veiller à ce qu'il soit indépendant des réseaux publics et prendre les mesures de sécurité et de protection qui s'imposent pour protéger ce réseau par la mise en place de dispositifs de cryptage, de protection et de vérification d'accès notamment;

i) Renforcer la coopération entre équipes d'intervention informatique d'urgence pour ce qui est de repérer les failles, d'instaurer des procédures de protection et de combler les lacunes;

j) Diffuser les procédures de sécurité et les méthodes pour remédier aux failles.

L'accent a été mis sur les moyens de mettre l'informatique et les communications au service du développement durable, en particulier dans les régions pauvres et reculées, comme suit :

a) Accélérer la marche vers l'élimination de la pauvreté, notamment grâce aux services bancaires mobiles qui ont déjà apporté dans le monde des avantages immédiats et palpables à des millions de personnes n'ayant aucune expérience en matière bancaire;

b) Atténuer les effets de la famine grâce aux nouvelles technologies et aux nouveaux moyens de communication qui offrent aux agriculteurs des informations cruciales et les aident à prendre les bonnes décisions concernant leurs produits agricoles.

La Jordanie recommande :

a) La mise sur pied d'équipes internationales chargées d'intervenir en cas de failles à la sécurité informatique, d'aider à les surmonter et de faire face aux catastrophes et aux crises informatiques;

b) L'intégration d'un représentant jordanien au Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui a été créé en 2003;

c) La promotion de la coopération scientifique et des possibilités de formation entre les pays membres du Conseil de sécurité.

Madagascar

[Original: français]
[20 juin 2017]

Les recommandations de l'Organisation des Nations Unies reposent sur la sécurité internationale et envisagent :

– La poursuite des études destinées à renforcer la sécurité des systèmes informatiques mondiaux et des systèmes mondiaux de télécommunication;

– L'évaluation de toutes les menaces qui existent ou pourraient exister dans le domaine de la sécurité informatique et l'adoption des stratégies appropriées face à ce fléau;

– L'engagement des responsables étatiques en faveur du renforcement de la sécurité informatique, en vue de dégager une vision commune de la sécurité à l'échelle mondiale;

La résolution 71/28 concerne spécifiquement le domaine de l'informatique et des télécommunications, domaine en plein essor à Madagascar. La réponse relative à cette résolution nécessite l'avis des experts dans ce domaine.

Norvège

[Original : anglais]
[27 juillet 2017]

La Norvège est un des pays les plus numérisés au monde et est de plus en plus tributaire d'un cyberespace sûr et efficace. Elle est fermement attachée à un cyberespace libre, ouvert, pacifique et sûr, afin que les avantages économiques et sociaux qui en découlent soient protégés et disponibles pour tous. Le cyberespace ne connaissant pas de frontières nationales, la sécurité ne peut y être assurée qu'à l'échelle internationale, grâce à une coopération étroite entre les États et le secteur privé.

Efforts déployés pour renforcer la sécurité informatique

Stratégies nationales

Le Gouvernement a publié un livre blanc, intitulé « Sécurité informatique : une responsabilité commune » (2016-2017), qui prévoit un cadre national destiné à renforcer la coordination entre les acteurs concernés au niveau national et la création d'une plateforme technique visant à améliorer la mise en commun d'informations entre entités publiques et privées.

Le 31 mars 2017, un centre de coordination combiné de cybersécurité a été créé pour les services de renseignement et de sécurité.

Stratégies internationales

Le Gouvernement a publié, dans le cadre de sa politique étrangère (2014-2015), un livre blanc sur les défis mondiaux en matière de sécurité, où les menaces cybernétiques occupent une place importante.

La Norvège s'apprête à lancer une stratégie internationale relative au cyberespace pour le pays.

Elle participe à plusieurs initiatives régionales de coopération sur les questions cybernétiques, notamment :

a) Le travail accompli à l'Organisation pour la sécurité et la coopération en Europe (OSCE) dans le domaine de l'élaboration de normes et de mesures de confiance en vue de réduire les risques de conflit liés à l'utilisation des technologies de l'information et de la communication;

b) Une coopération étroite avec le Centre d'excellence pour la cyberdéfense de l'Organisation du Traité de l'Atlantique Nord à Tallin, y compris pour l'application du droit international dans le cyberespace et l'élaboration de la doctrine;

c) La Convention du Conseil de l'Europe sur la cybercriminalité.

La Norvège appuie les travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

Elle prend part à des dialogues bilatéraux et régionaux sur les questions cybernétiques, notamment avec les autres pays nordiques.

Mesures que la communauté internationale pourrait prendre pour renforcer la sécurité informatique à l'échelle mondiale

La Norvège considère que le droit international s'applique au cyberespace et que l'adhésion des États à ses principes, notamment les obligations découlant de la Charte des Nations Unies, représente un cadre essentiel pour guider l'utilisation qu'ils font des technologies de l'information et de la communication. La communauté internationale doit étudier plus avant l'application du droit international au numérique ainsi que les normes d'un comportement responsable dans le cyberespace.

La viabilité mondiale de l'Internet dépend de l'équilibre entre ouverture, sécurité, robustesse et liberté, qui ne peut être assuré que par la coopération internationale et le dialogue, aux niveaux international et régional. Il conviendra ainsi de poursuivre les travaux en cours à cet égard dans des instances telles que l'ONU, l'Union européenne, l'Organisation de coopération et de développement économiques et l'OSCE.

Les droits fondamentaux universels s'appliquent aussi dans le cyberespace. Les droits dont jouissent les personnes hors ligne doivent également être protégés en ligne, en particulier la liberté d'expression, notamment la liberté de rechercher et de partager des informations, et le droit à la vie privée.

Paraguay

[Original : espagnol]
[31 juillet 2017]

Le Paraguay estime, lui aussi, que la sécurité informatique acquiert une importance croissante au niveau mondial puisque les gouvernements sont de plus en plus dépendants du cyberespace et des technologies de l'information et de la communication. La riposte à l'évolution des cyberattaques doit donc être conjointe, dynamique et proportionnée. Si des mesures stratégiques ne sont pas prises à l'échelle mondiale, les actions entreprises par un seul pays en matière de cybersécurité ne seront que sporadiques, peu viables, redondants et, au final, inefficaces.

Afin de renforcer la sécurité informatique au niveau national, le Gouvernement paraguayen a adopté, en avril 2017, un plan national sur la cybersécurité auquel des représentants de tous les secteurs ayant un rôle et des intérêts dans ce domaine ont participé. Ce plan sert de base aux décisions gouvernementales et nationales consacrées à la question et définit dans les grandes lignes les mesures que le pays doit prendre pour renforcer la sécurité de ses moyens essentiels et pour réaliser l'objectif d'un cyberespace sûr, fiable et résistant. Les infractions relevant de la cybercriminalité sont recensées dans le droit pénal interne. Le Paraguay accueille depuis cinq ans un congrès ibéro-américain sur la sécurité informatique, créé en vue de faire connaître les innovations dans ce domaine, de mettre en commun des données d'expérience et d'examiner les solutions aux technologies de l'information et de la communication.

Au niveau sous-régional, le Marché commun du Sud (MERCOSUR) compte sur une instance permanente, la *Reunión de Autoridades sobre Privacidad y Seguridad de la Información e Infraestructura Tecnológica del MERCOSUR* (Réunion des autorités sur la sécurité et le caractère privé des informations et de l'infrastructure technologique du MERCOSUR), chargée de proposer des mesures et initiatives communes dans le domaine de la cybersécurité. Au niveau régional, les Amériques disposent d'une stratégie intégrale de cybersécurité interaméricaine,

fondée sur le principe que tous les utilisateurs des réseaux et systèmes d'information doivent être conscients de leurs fonctions et responsabilités en matière de sécurité, afin de créer une culture de la cybersécurité.

Afin d'établir un cadre efficace pour la protection des réseaux et des systèmes d'information au niveau mondial, notamment l'Internet, et de réagir aux situations critiques et les surmonter, la communauté internationale devra :

– Informer les utilisateurs afin qu'ils protègent leurs systèmes informatiques contre les risques et les menaces;

– Améliorer l'éducation et la prise de conscience dans le cadre d'associations publiques et privées;

– Définir et évaluer les normes techniques et les meilleures pratiques pour assurer la sécurité des informations diffusées par les réseaux de communication, et en promouvoir l'adoption;

– Promouvoir l'adoption de stratégies et de lois sur les infractions relevant de la cybercriminalité afin de protéger les utilisateurs et de prévenir et empêcher l'usage abusif ou illicite du matériel informatique, tout en respectant les droits des utilisateurs.

Pays-Bas

[Original : anglais]
[31 mai 2017]

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 71/28.

Le cyberespace, en particulier l'Internet, constitue une ressource essentielle pour la croissance de l'économie et de la société. L'importance croissante qu'il revêt suscite des défis nouveaux pour la communauté mondiale. Les sociétés, fortement interconnectées, dépendent de l'Internet et des technologies de l'information et de la communication et sont, de ce fait, devenues plus vulnérables à l'utilisation frauduleuse de ces technologies. Les tensions géopolitiques se manifestent de plus en plus dans le cyberespace et les États et autres acteurs politiques y mènent de plus en plus d'activités pour servir leurs intérêts stratégiques. Toutefois, les activités dans le cyberespace peuvent être un facteur d'instabilité dans les relations internationales et représenter un risque pour la paix et la sécurité internationales.

Il est évident qu'une coopération internationale est nécessaire pour réduire ce risque. À la lumière de ce qui précède, les Pays-Bas ont intensifié leur participation à la diplomatie en ligne pour maintenir la paix et la stabilité dans le cyberespace, promouvoir l'ordre juridique international et favoriser une culture de collaboration en faveur de la sécurité, comme le pays l'a indiqué dans sa cyberstratégie *Building Digital Bridges* (« Combler le fossé numérique »).

La communauté internationale prend des mesures pour parer les risques. Les rapports publiés par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale ont une grande importance à cet égard. Les Pays-Bas sont également reconnaissants d'être en mesure de contribuer aux travaux de 2017 du Groupe d'experts gouvernementaux.

Les Pays-Bas continuent de promouvoir un dialogue sans exclusive sur le comportement responsable des États dans le cyberespace, défendant les droits de

l'homme en ligne et favorisant le renforcement des capacités grâce à diverses activités, notamment :

a) Dans la meilleure tradition de leur appui au développement de l'ordre juridique international, les Pays-Bas ont organisé des consultations entre les conseillers juridiques des États sur le *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Manuel de Tallinn 2.0 relatif au droit international applicable aux opérations cybernétiques);

b) Les Pays-Bas ont aidé l'Institut des Nations Unies pour la recherche sur le désarmement à organiser une série de trois ateliers sur les normes numériques, le droit international et la lutte contre la diffusion de techniques et d'outils malveillants. Ces ateliers ont rassemblé de manière fructueuse des diplomates et des membres de la communauté technique;

c) Enfin, les Pays-Bas ont lancé de nombreuses initiatives visant à favoriser l'adoption de normes directives, y compris dans le cadre de la Commission mondiale sur la stabilité du cyberespace (« *Global Commission on the Stability of Cyberspace* »), qui élaborera des propositions concernant les normes et les politiques visant à renforcer la sécurité et la stabilité internationales.

Toutes ces mesures visent à rendre les relations internationales numérisées et le cyberespace lui-même plus stables et plus sûrs; les Pays-Bas estiment qu'elles sont essentielles si l'on veut réduire les risques de conflit et maintenir un cyberespace ouvert, libre et sûr.

Portugal

[Original : anglais]
[27 juillet 2017]

Dans sa résolution 71/28, intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », l'Assemblée générale a rappelé le rôle de la science et de la technique dans le contexte de la sécurité internationale, et a notamment constaté que les innovations dans ces domaines pouvaient se prêter à des applications civiles aussi bien que militaires. Les progrès dans les domaines de l'information et des télécommunications signifient la multiplication des possibilités de développement des connaissances, la coopération entre États, le renforcement du potentiel créatif de l'humanité et la circulation de l'information dans la communauté mondiale. Toutefois, le Portugal estime que ces technologies et moyens risquent d'être utilisés à des fins incompatibles avec le maintien de la stabilité et de la sécurité internationales et de porter atteinte à l'intégrité des États.

Dans sa résolution 71/28, l'Assemblée a prié les États Membres de communiquer des informations dans les quatre domaines suivants :

a) L'ensemble des questions qui se posent en matière de sécurité informatique;

b) Les actions engagées au niveau national pour renforcer la sécurité informatique et promouvoir la coopération internationale dans ce domaine;

c) Le contenu des principes destinés à renforcer la sécurité des systèmes mondiaux de télécommunication;

d) Les mesures que la communauté internationale pourrait prendre pour renforcer la sécurité informatique à l'échelle mondiale.

Dans son rapport de 2013 (A/68/98), le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale propose des recommandations dans les domaines suivants : normes, règles et principes de comportement responsable des États; mesures visant à instaurer la confiance et échange d'informations; mesures de renforcement des capacités.

Partant de ces recommandations, le Portugal fait part de ses observations, comme suit.

Normes, règles et principes de comportement responsable des États

Le Portugal considère que la sécurité de l'information en réseau revêt une importance croissante.

Il est important de redoubler d'efforts pour faire appliquer la législation en matière de sécurité et d'intégrité des réseaux, en adoptant des méthodes d'évaluation des risques, lesquelles requièrent que soient adoptées des mesures de sécurité adaptées sur les plans technique et organisationnel et qui comprennent l'obligation de signaler les violations de la sécurité ou les atteintes à l'intégrité ayant des répercussions importantes sur le fonctionnement des services.

S'agissant des principes, il est important de renforcer l'idée que la réglementation doit découler de règles internationales.

Au niveau international, il importe de renforcer la mise en commun des informations et d'effectuer des exercices d'entraînement sur le terrain dans les zones frontalières.

Mesures de renforcement de la confiance et mise en commun des informations

Il est indispensable d'encourager la mise en commun des informations parmi toutes les parties prenantes (publiques et privées) en tenant compte du contexte plus vaste de la mondialisation.

Les efforts déployés par le Portugal au niveau national ont porté essentiellement sur l'exécution d'exercices conjoints auxquels ont participé des entités publiques et privées, la promotion de la normalisation technique et l'organisation de conférences et de séminaires auxquels sont parfois invités des conférenciers internationaux.

Mesures de renforcement des capacités

Il importe de mettre en place des mesures de renforcement des capacités, même si la formation des ressources humaines nécessaires pour ces activités présente des difficultés.

Il convient de faciliter l'accès aux connaissances et de promouvoir l'instruction collective dans plusieurs domaines, notamment la sécurité, auprès de toutes les parties prenantes principales.

Qatar

[Original : anglais]
[4 mai 2017]

L'État du Qatar a déclaré en son temps que la sécurité informatique, ou cybersécurité, était non seulement une question technique, mais également un enjeu de politique nationale. C'est pourquoi, il a créé, en 2005, une équipe d'intervention

informatique d'urgence (voir www.qcert.org) chargée de stimuler le changement et, plus précisément, d'accélérer l'adoption généralisée de pratiques et de politiques efficaces en matière de cybersécurité; l'équipe est désormais chargée au niveau national de protéger les ressources numériques de l'État du Qatar.

En 2013, le Premier Ministre a constitué un Comité de la cybersécurité, qui a élaboré une stratégie nationale censée améliorer les conditions de sécurité au Qatar et garantir l'essor continu de la nation, et s'appuyant sur cinq piliers destinés à permettre de:

- Protéger les infrastructures d'information nationales essentielles;
- Réagir aux attaques et situations de crise cybernétique, les enrayer et les surmonter grâce à une mise en commun des informations, à une collaboration et à une action opportunes;
- Mettre en place un cadre juridique et réglementaire pour un cyberespace sûr et dynamique;
- Promouvoir une culture de la cybersécurité qui favorise une utilisation sûre et appropriée du cyberespace;
- Renforcer et cultiver les capacités nationales en matière de cybersécurité.

L'équipe d'intervention informatique d'urgence a pu ainsi offrir divers services de sécurité des informations répondant aux besoins des habitants, des entreprises et des organisations du pays, en particulier dans les domaines suivants : intervention en cas de crise, renseignement, résilience, formation et sensibilisation, gestion des crises, recensement des principales infrastructures publiques et attribution de licences pour celles-ci, et création d'un cadre national pour l'application des règles de sécurité de l'information.

Le Qatar estime qu'actuellement, les États ne sont pas suffisamment au fait en mesure d'acquérir une conscience de la situation dans le domaine cybernétique et sont peu outillés pour l'expliquer aux niveaux régional et international de façon à permettre une prise de décisions efficace. Il faut donc poursuivre les travaux sur la prévention collaborative pour renforcer la cybersécurité dans les services et infrastructures numériques afin de garantir la résilience, en particulier en ce qui concerne les opérations quotidiennes des gouvernements, des services, des entreprises, des consommateurs et des citoyens.

La cybersécurité n'est jamais plus efficace que lorsque les informations sont mises en commun. Les États auront tout intérêt à élaborer des accords sur le partage de l'information grâce à des cadres de collaboration décrivant des méthodes de vérification et d'observation.

Des attaques ne manqueront pas de se produire et les nations, les gouvernements, les organisations et les entreprises doivent, ensemble, se préparer à les affronter.

Singapour

[Original : anglais]
[31 juillet 2017]

Petit État très connecté, Singapour œuvre en faveur d'un cyberespace sécurisé et résilient, conforme au droit international; préconise des normes bien définies de comportement responsable des États, et appuie les actions coordonnées de renforcement des capacités destinées à assurer le respect de ces normes. Si l'on veut

relever les nouveaux défis que posent les menaces cybernétiques, il faudra instaurer une solide coopération internationale – à laquelle Singapour ne manquera pas de prendre part.

En 2015, Singapour a créé une agence de cybersécurité chargée d'assurer un contrôle centralisé des fonctions de cybersécurité. En octobre 2016, Singapour a lancé sa stratégie de cybersécurité, qui met l'accent sur sa méthode globale pour protéger les services essentiels des menaces cybernétiques et créer un cyberespace sûr. Cette stratégie s'appuie sur quatre piliers : l'élaboration d'une infrastructure résiliente, la création d'un cyberespace plus sûr, le développement d'un système de cybersécurité dynamique et le renforcement des partenariats existants.

Au niveau régional, Singapour s'emploie à renforcer et approfondir les capacités existantes, en collaboration avec les États voisins. Le pays a lancé, en collaboration avec l'Association des nations de l'Asie du Sud-Est (ASEAN), un programme de renforcement des capacités cybernétiques, d'une valeur de 10 millions de dollars singapouriens, destiné à compléter les mesures régionales entreprises dans ce domaine. Dans le cadre de ce programme, Singapour a organisé, en mai 2017, un atelier de l'ASEAN sur les normes cybernétiques et a prévu d'accueillir, en août 2017, un atelier de l'ASEAN pour le renforcement des capacités en matière de cybersécurité. Le pays est également l'hôte, chaque année, de la Cybersemaine internationale de Singapour, qui comprend une conférence ministérielle de l'ASEAN sur la cybersécurité et le Colloque international des responsables de la cybersécurité permettant aux administrateurs des gouvernements, aux entreprises et aux milieux universitaires du monde d'examiner les questions nouvelles et interdisciplinaires et d'y associer la région.

En ce qui concerne la coopération multilatérale, Singapour appuie les travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, notamment les 11 normes énumérées dans son rapport de 2015. Il est important de définir et d'appliquer ces normes largement reconnues, en particulier les normes opérationnelles. Ces normes exigent, notamment, de s'abstenir de soutenir les activités en ligne qui visent à endommager les infrastructures essentielles ou qui empêchent les équipes d'intervention de répondre aux atteintes à la sécurité informatique, et de renoncer à se servir de ces équipes d'intervention pour se livrer à des activités internationales malveillantes.

Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

[Original : anglais]
[31 juillet 2017]

Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord se félicite de l'occasion qui lui est donnée de donner suite à la résolution 71/28 de l'Assemblée générale, intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », dans le sillage de sa contribution concernant la résolution 70/237 de 2016. Pour éviter tout risque de confusion, en raison des interprétations différentes données à l'expression « sécurité informatique », le Royaume-Uni préfère employer dans ce contexte le terme « cybersécurité » et les concepts y afférents.

Le Royaume-Uni est conscient du fait que le cyberespace constitue un élément fondamental de la sécurisation des infrastructures nationales et internationales vitales et qu'il est le socle essentiel des activités économiques et sociales en ligne. Les menaces, réelles ou potentielles, associées aux activités menées dans le

cyberespace sont toujours très préoccupantes. La nouvelle stratégie nationale de cybersécurité, publiée en octobre 2016, orientera les efforts que le pays déploiera au cours des cinq prochaines années pour défendre ses ressources, dissuader ses adversaires et développer le secteur de la cybersécurité.

Le Royaume-Uni continue de jouer un rôle de premier plan dans le débat international sur la cybersécurité. Il a détaché des experts aux cinq Groupes d'experts gouvernementaux chargés d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Malgré l'absence de consensus au sein du Groupe de 2017, le pays s'est engagé à promouvoir un cadre international pour la stabilité du cyberespace fondé sur l'application du droit international existant et est convenu de normes de comportement responsable des États et de mesures de confiance, appuyées par des programmes coordonnés de renforcement des capacités. Le Royaume-Uni se félicite également du fait que l'Organisation pour la sécurité et la coopération en Europe et d'autres instances régionales se soient efforcées de faire des propositions pour la mise en œuvre de mesures de confiance, et continuera de montrer l'exemple en adoptant de telles mesures.

La présente réponse expose les efforts que déploie le Royaume-Uni pour soutenir et améliorer la cybersécurité et l'échange de bonnes pratiques, aux niveaux national et international, en collaborant avec des partenaires internationaux dans la lutte contre la cybercriminalité et le traitement des principaux incidents et en renforçant les capacités dans ce domaine. Le Royaume-Uni attend avec intérêt la poursuite des progrès dans tous ces domaines et se réjouira de s'y associer activement. Il continuera de participer pleinement au renforcement des capacités et à la coopération internationale en matière de cybersécurité.

Turquie

[Original : anglais]
[31 juillet 2017]

Les technologies de l'information et de la communication sont devenues des éléments essentiels de la vie économique et de la société d'aujourd'hui. Elles contribuent à la richesse sociale et au développement et font partie du quotidien. Largement utilisées, notamment par les secteurs public et privé, les infrastructures essentielles et les individus, elles se sont généralisées dans le pays et le monde, malgré les risques liés à la cybersécurité.

C'est pourquoi, la Turquie a pris part à de nombreuses initiatives de coopération sur des questions liées à la cybersécurité, dans le but d'assurer la cybersécurité. Dans ce contexte, sous la coordination du Ministère des transports, des affaires maritimes et des communications, des exercices sur la cybersécurité ont été organisés à l'échelle nationale. Le premier exercice international sur un bouclier cybernétique a été effectué à Istanbul, où la Turquie participe et contribue régulièrement, chaque année, aux activités internationales liées à la cybersécurité, à savoir la Coalition cybernétique, l'exercice Locked Shields et l'exercice de gestion des crises de l'Organisation du Traité de l'Atlantique Nord (OTAN).

Le dialogue et la coopération avec l'ONU, l'OTAN, l'Union européenne, l'Organisation pour la sécurité et la coopération en Europe et d'autres organisations internationales ou non gouvernementales, les milieux universitaires et les faiseurs d'opinion, ont été améliorés. Cette démarche est renforcée par des conférences, des cours, des séminaires, des réunions, des programmes d'enseignement supérieur et

autres programmes de soutien. La Turquie se trouve à la pointe de l'action régionale en matière de cybersécurité en concluant des accords bilatéraux avec divers États.

Le mémorandum d'accord décrivant la coopération entre l'OTAN et ses alliés a été approuvé par le Comité de cyberdéfense de l'OTAN, et des travaux connexes sont en cours en vue de sa signature. La Turquie est au nombre des nations qui appuient le Centre d'excellence de l'OTAN pour la cyberdéfense. Elle suit les travaux du Comité des plans d'urgence dans le domaine civil de l'OTAN et les réunions du Centre régional de vérification et d'assistance à la mise en œuvre en matière de contrôle des armes – Centre pour la coopération en matière de sécurité , établissant une coopération sur diverses questions. Un des fondateurs du Forum international sur le cyberespace, la Turquie est devenue partie au document-cadre et à la Déclaration de La Haye sur le Forum international.

Une décision sur la cybersécurité, mettant l'accent sur le travail du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, a été prise lors du sommet du Groupe des 20, qui s'est tenu en Turquie les 15 et 16 novembre 2015.

La Convention du Conseil de l'Europe sur la cybercriminalité a été signée par la Turquie à Strasbourg en 2010, approuvée par la loi n° 6533 de 2014 puis transposée dans la législation nationale.

Une stratégie et un plan d'action nationaux en matière de cybersécurité pour la période 2016-2019 ont été élaborés grâce à la collecte, à l'examen et à l'évaluation des informations générées dans le cadre de réunions et de plateformes.

Il est essentiel pour tous de renforcer la sécurité de l'information au niveau mondial et, par là même, d'instaurer une culture de la sécurité au sein de la communauté internationale. Dans le même temps, dans le but de préserver sa sécurité nationale, tout État a le droit de prendre des mesures pour se protéger contre l'utilisation malveillante des technologies de l'information et des communications par des terroristes, des extrémistes, des groupes criminels organisés et des pirates indépendants. Il est également essentiel, dans ce contexte, de renforcer la législation internationale et les accords internationaux bilatéraux.