Nations Unies A/70/172

Assemblée générale

Distr. générale
22 juillet 2015
Français
Original : anglais/arabe/espagnol

Soixante-dixième session
Point 93 de l'ordre du jour provisoire*

Progrès de l'informatique et des télécommunications et sécurité internationale

Rapport du Secrétaire général

Table des matières

* A/70/150.

15-12333 (F) 240815 240815

I. Introduction

1. Le 2 décembre 2014, l'Assemblée générale a adopté la résolution 69/28 intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale ». Au paragraphe 3 de cette résolution, l'Assemblée invite tous les États Membres à continuer de communiquer au Secrétaire général, en tenant compte des constatations et recommandations figurant dans le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (A/68/98), leurs vues et observations sur les questions suivantes :

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

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

c) Les 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. Pour donner suite à cette demande, une note verbale a été adressée aux États Membres le 2 février 2015 pour les inviter à communiquer des informations à ce sujet. Les réponses reçues jusqu'à présent sont reproduites dans la section II ci-dessous. Les autres réponses reçues seront publiées sous forme d'additifs au présent rapport.

II. Réponses reçues des gouvernements

Allemagne

[Original : anglais]
[27 mai 2015]

Un Internet libre, ouvert à tous, sécurisé et sûr offre de vastes possibilités de croissance économique, de développement social et de progrès scientifique ainsi que de promotion de la démocratie, de la bonne gouvernance et de l'état de droit. Parallèlement, les inquiétudes quant aux risques que présente le cyberespace pour la sécurité internationale ne cessent de croître. Au cours des derniers mois, on a constaté une augmentation des attaques de logiciels malveillants contre des cibles très exposées, telles que les organes de presse. Ce sont surtout les attaques contre les principales infrastructures qui pourraient avoir de graves conséquences.

Une cyberguerre totale semble peu probable à l'heure actuelle. Par contre, aujourd'hui, des moyens cybernétiques limités peuvent réellement être utilisés dans le cadre d'une guerre, y compris lors de conflits hybrides. De plus, il existe le danger que des attaques informatiques ne dégénèrent en véritable conflit.

L'Allemagne préconise une approche en trois volets pour agir dans cet environnement : convenir de règles adaptées à un comportement responsable de

l'État dans le cyberespace, établir des mesures de confiance et renforcer la résilience informatique.

Les Nations Unies sont le lieu essentiel pour mettre en place les règles de comportement responsable des États dans le cyberespace. Le consensus du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale de 2012-2013, selon lequel le droit international, surtout la Charte des Nations Unies, s'applique au cyberespace, est un point de départ important. Le Groupe d'experts gouvernementaux de 2014-2015, auquel l'Allemagne a une fois de plus pris part activement, s'est basé sur ce point.

Une vision commune des règles, normes et principes de comportement responsable des États dans le cyberespace pourrait permettre d'améliorer la transparence et la prévisibilité internationales et de contribuer dès lors à la paix et à la stabilité. Il serait par exemple utile d'avoir une meilleure vision commune de la manière dont les lois sur les conflits armés s'appliquent à l'utilisation des moyens cybernétiques militaires que de plus en plus d'États mettent au point.

En ce qui concerne le renforcement de la confiance, l'Allemagne attache la plus haute importance aux organisations régionales. En 2013, l'Organisation pour la sécurité et la coopération en Europe a convenu d'une première série de mesures de renforcement de la confiance cybernétique. La mise en œuvre de ces mesures progresse de manière satisfaisante et des négociations sont en cours en vue d'une deuxième série, qui porterait sur le renforcement de la confiance et sur la coopération. Dans le cadre de sa future présidence de l'Organisation, l'Allemagne prévoit de donner la priorité à la cybersécurité.

L'Allemagne est en train d'élaborer une loi sur la sécurité des technologies de l'information visant à renforcer la résilience informatique à l'échelle nationale. Le projet de texte de cette loi définit les exigences minimales relatives à la sécurité des technologies de l'information des infrastructures essentielles. Il mentionne qu'il est obligatoire de signaler les incidents majeurs dans le but d'améliorer la sécurité globale des systèmes et la protection du public en général. L'Allemagne propose également d'aider d'autres États à renforcer leurs capacités de gestion des risques liés à la cybersécurité.

On trouvera le texte intégral de la réponse de l'Allemagne à l'adresse suivante : www.un.org/disarmament/topics/informationsecurity/.

Canada

[Original : anglais]
[4 juin 2015]

Le cyberespace a renforcé les interactions sociales et transformé le secteur privé et les gouvernements et il continue d'être moteur de croissance économique, d'innovation et de développement social. Il a aussi créé des menaces et des difficultés nouvelles pour notre société.

Le Canada souligne à nouveau que, dans le rapport de 2013 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, les États ont

clairement affirmé que l'application du droit international au cyberespace était un élément essentiel pour définir des règles et des principes favorisant un comportement responsable des États, et il encourage les États à travailler à l'avenir à l'élaboration de normes applicables en temps de paix.

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. Les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne.

Le Canada souscrit à l'objectif d'un Internet libre, ouvert à tous et sûr, et il veut en venir à cette fin par les moyens suivants :

a) L'application de la Stratégie de cybersécurité et du Plan d'action du Canada reste un des efforts prioritaires au niveau national. Ces deux mesures contribuent à sécuriser les systèmes cybernétiques du pays et à protéger les Canadiens en ligne grâce à la collaboration active des secteurs des infrastructures essentielles (par exemple, les finances, les transports et l'énergie);

b) Le Canada a mis au point un cadre de gestion des incidents cybernétiques, qui permet de gérer et de coordonner, à l'échelle nationale et de façon consolidée, les menaces ou les incidents cybernétiques réels ou potentiels;

c) La nouvelle législation canadienne antipourriel permet de préciser les droits et obligations ainsi que les responsabilités de chaque organisme public, et permet de renforcer l'application des dispositions législatives et la collaboration internationale;

d) Au niveau international, le Canada a investi 8 millions de dollars canadiens pour appuyer des projets de renforcement des capacités en matière de cybersécurité, principalement sur le continent américain et en Asie du Sud-Est. Le Canada a également versé plus de 3,6 millions de dollars canadiens à l'Organisation des États américains pour la période 2007-2016 en vue de renforcer les capacités des pays membres de l'Organisation, y compris en mettant en place des équipes d'intervention en cas de cyberincidents. Le Canada est également membre fondateur du Forum international sur le cyberespace;

e) Le Canada 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;

f) Le Canada collabore avec le Forum régional de l'Association des nations de l'Asie du Sud-Est en vue de renforcer les capacités en matière de mesures de confiance et de transparence, qui sont essentielles à la stabilité du cyberespace;

g) Dans le cadre du Plan d'action sur la cybersécurité élaboré par le Canada et les États-Unis, les deux pays collaborent pour accroître la résilience de la cyberinfrastructure canadienne et améliorer l'engagement, la collaboration et l'échange d'informations aux niveaux stratégique et opérationnel;

h) Le Canada participe aussi à des initiatives de lutte contre la cybercriminalité dans le cadre du Groupe des Sept, de l'Office des Nations Unies contre la drogue et le crime et de l'Organisation des États américains et de

l'Association des nations de l'Asie du Sud-Est, et le pays est membre de l'Alliance mondiale contre les abus sexuels commis contre des enfants via Internet;

i) Le Canada recommande que tous les États Membres désireux d'améliorer la cybersécurité et de prévenir la cybercriminalité se réfèrent à la Convention sur la cybercriminalité du Conseil de l'Europe.

On trouvera le texte intégral de la réponse du Canada à l'adresse suivante : www.un.org/disarmament/topics/informationsecurity/.

Cuba

[Original : espagnol]
[26 mai 2015]

Cuba partage la préoccupation exprimée dans la résolution 69/28 selon laquelle les technologies et moyens d'information 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 de l'infrastructure des États, nuisant ainsi à leur sécurité dans les domaines tant civil que militaire.

Cette résolution met également l'accent sur la nécessité de prévenir l'utilisation des moyens et des technologies d'information à des fins criminelles ou terroristes.

Dans ce contexte, Cuba se déclare très inquiet de l'emploi clandestin et illégal, par des individus, des organisations et des États, des systèmes informatiques d'autres nations contre des pays tiers, ce qui risque de provoquer des conflits internationaux.

Le seul moyen de prévenir et d'affronter ces menaces inédites ainsi que d'éviter que le cyberespace devienne un théâtre d'opérations militaires est la coopération étroite entre tous les États.

L'usage des télécommunications dans le but déclaré ou inavoué d'enfreindre l'ordre juridique et politique des États est une atteinte aux normes en la matière reconnues sur le plan international, dont les effets peuvent susciter des tensions et des situations défavorables à la paix et à la sécurité internationales.

Au 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 des pays d'Amérique latine et des Caraïbes ont proclamé que les régions d'Amérique latine et des Caraïbes étaient une zone de paix afin, entre autres, de susciter des relations d'amitié et de coopération entre eux et avec d'autres nations, indépendamment des différences existant entre leurs systèmes politiques, économiques et sociaux ou leurs niveaux de développement, de pratiquer la tolérance et de coexister en paix comme de bons voisins.

Lors du troisième Sommet de la CELAC, qui s'est tenu à Belén, au Costa Rica, les 28 et 29 janvier 2015, les États membres ont souligné que les technologies de l'information et des communications, y compris Internet, ainsi que l'innovation étaient des outils non négligeables pouvant encourager la paix et promouvoir le bien-être, le développement humain, les connaissances, l'inclusion sociale, la croissance économique, et ils ont rappelé qu'ils contribuaient à l'amélioration de la

portée et de la qualité des services sociaux. L'utilisation pacifique des technologies de l'information et des communications, conformément à la Charte des Nations Unies et au droit international, a été confirmée et les États ont souligné que ces technologies ne devraient jamais être utilisées dans l'optique de nuire à la société ou d'engendrer des situations pouvant créer des conflits entre États.

Néanmoins, ces efforts sont entravés par toutes les émissions de radio et de télévision diffusées par le Gouvernement des États-Unis contre Cuba, en violation des buts et principes de la Charte des Nations Unies et de divers règlements de l'Union internationale des télécommunications. En outre, et c'est tout aussi important, ces programmes portent atteinte à la souveraineté de Cuba.

Cuba rappelle qu'il est illégal d'avoir recours à l'information comme outil de propagande ou de déstabilisation dans le but affiché de compromettre l'ordre interne d'autres États, de violer leur souveraineté et de commettre des actes d'immixtion et d'ingérence dans leurs affaires intérieures et que de telles pratiques doivent cesser.

Nous réexprimons notre rejet catégorique de l'usage des technologies de l'information et des communications contraire au droit international, et de toutes les actions de ce type. Nous soulignons qu'il importe de veiller à ce que leur usage soit pleinement compatible avec les buts et principes de la Charte des Nations Unies et du droit international, en particulier la souveraineté, la non-ingérence dans les affaires intérieures et les règles de coexistence entre les États reconnues sur le plan international.

Cuba réaffirme que la coopération internationale est essentielle pour faire face aux dangers associés à l'utilisation abusive des technologies de l'information et des communications. Cuba souligne également l'importance de l'Union internationale des télécommunications dans le cadre des débats intergouvernementaux sur les questions de cybersécurité.

Cuba espère que le nouveau contexte de ses relations bilatérales avec les États-Unis, annoncé le 17 décembre 2014 par les Présidents Raúl Castro Ruz et Barack Obama, y compris la décision de rétablir les relations diplomatiques entre les deux pays et d'engager un processus visant à normaliser les relations, mettra un terme à ces politiques d'agression et que l'embargo économique, commercial et financier qui est à l'origine des graves souffrances du peuple cubain sera levé. L'embargo a eu des conséquences néfastes dans le domaine de l'information et des communications et dans d'autres domaines liés à la vie quotidienne du peuple cubain.

Dans le cadre du programme d'informatisation de Cuba, le premier atelier national sur l'informatisation et la cybersécurité, sur le thème « Devenir une société informatisée », s'est tenu du 18 au 20 février 2015. Plus de 11 500 professionnels des technologies de l'information et des communications venus de tout le pays ont participé à cet événement. Un des thèmes de l'atelier était la question de la sécurité, du contrôle et de la gestion des technologies de l'information et des communications.

Cuba a créé le Conseil de l'informatisation et de la cybersécurité, dirigé par l'organe suprême de l'État, le Gouvernement et le Parti communiste cubain, qui a pour fonctions de recommander, de coordonner et de superviser l'ensemble des politiques et stratégies en faveur de ce processus. Le pays travaille également à la création de l'union des informaticiens de Cuba.

Cuba a appuyé la résolution 69/28 et continuera à participer au développement mondial et pacifique des technologies de l'information et des télécommunications et à leur emploi pour le bien de toute l'humanité.

El Salvador

[Original : espagnol]
[21 avril 2015]

Dans le cadre de leur dispositif de sécurité de l'information et des télécommunications, les forces armées d'El Salvador ont centralisé les télécommunications orales, audiovisuelles et électroniques, qui sont indépendantes du réseau public. Un périmètre de sécurité informatique a été créé et configuré; en outre, il existe un système de cryptage pour la gestion d'informations officielles afin de protéger toute l'information contre tout agent extérieur qui voudrait y accéder et contre les attaques cybernétiques.

Espagne

[Original : espagnol]
[29 mai 2015]

L'Espagne considère que les technologies de l'information et des communications apportent un appui essentiel aux sociétés partout dans le monde, mais que la mondialisation de ces technologies entraîne de graves risques et menaces comme le cyberespionnage, le cyberterrorisme, le cyberactivisme et la cyberguerre.

Après avoir créé un Conseil national de la cybersécurité, l'Espagne a continué à faire des progrès dans l'élaboration de plans découlant de la stratégie nationale de cybersécurité, en vue de renforcer les capacités de prévention, de protection, de détection, d'analyse, d'intervention, de rétablissement et de coordination face aux menaces cybernétiques.

L'Espagne continue de participer activement à la promotion de la coopération internationale et suit de près toutes les initiatives stratégiques ayant des incidences sur la cybersécurité tant au sein de l'Union européenne que de grands forums internationaux tels que l'Organisation pour la sécurité et la coopération en Europe, l'Organisation du Traité de l'Atlantique Nord et le Conseil de l'Europe.

L'Espagne ne cesse de souligner l'importance du rôle des Nations Unies pour parvenir à un consensus international sur les problèmes de cybersécurité et elle préconise la poursuite d'un dialogue institutionnalisé auquel participeraient d'autres instances internationales afin de promouvoir la coopération régionale et la mise en place de normes mondiales, de meilleures pratiques, de règles de conduite entre les États et de mesures de renforcement de la confiance, l'objectif ultime étant de garantir une utilisation pacifique et sûre des technologies de l'information.

L'Espagne estime que les États devraient parvenir à un consensus dans quatre domaines. Tout d'abord, ils devraient mettre en place des mesures de renforcement de la confiance de type coopératif avec pour objectif ultime de promouvoir la

transparence entre les États dans le domaine de la cybersécurité et de renforcer leurs capacités de neutraliser les éventuelles attaques provenant de pays tiers.

Deuxièmement, l'Espagne considère que les États devraient continuer à réfléchir sur la manière dont les principes et normes du droit international devraient être interprétés et appliqués dans le cyberespace; en particulier ceux qui ont trait à la menace ou à l'emploi de la force, au droit humanitaire et à la protection des libertés et droits fondamentaux de la personne.

Troisièmement, l'Espagne considère qu'il faut renforcer la coopération internationale en améliorant les voies de communication, en mettant en place des mécanismes de coordination des équipes d'intervention informatique d'urgence, en menant des exercices conjoints et d'autres opérations similaires et en faisant la promotion de mécanismes de coopération judiciaire et policière.

Enfin, il faudrait continuer à encourager le renforcement des capacités dans les pays où cela s'avère nécessaire et à prêter assistance aux États bénéficiaires pour les aider à élaborer des lois nationales définissant des normes en matière de cybersécurité.

On trouvera le texte intégral de la réponse de l'Espagne à l'adresse suivante : www.un.org/disarmament/topics/informationsecurity/.

Géorgie

[Original : anglais]
[26 mai 2015]

Le Gouvernement géorgien place l'information et la cybersécurité au centre de ses préoccupations politiques et considère que la lutte contre les menaces cybernétiques fait partie intégrante de la politique de sécurité nationale, en particulier compte tenu des vastes réformes menées dans l'ensemble du pays dans le domaine du cybergouvernement et de la dépendance croissante de ses principales infrastructures envers les technologies de l'information et des communications. En exprimant ces préoccupations, le Gouvernement géorgien a introduit plusieurs mesures stratégiques, juridiques, organisationnelles et institutionnelles afin de renforcer la sécurité de l'information.

La première stratégie portant sur la cybersécurité à l'échelle nationale est énoncée dans la stratégie de cybersécurité et dans le plan d'action pour 2013-2015, qui est le principal document énonçant la politique de l'État dans le domaine de la cybersécurité, y compris les objectifs stratégiques et les principes directeurs, et définissant les points d'intervention et les tâches à accomplir. La cybersécurité est l'une des principales priorités de la politique de sécurité du pays et la protection du cyberespace est considérée comme un élément aussi important pour la sécurité nationale que la protection du sol, de l'eau et de l'espace aérien.

Une autre étape de l'institutionnalisation de la sécurité de l'information fut, en 2010, la création, au Ministère de la justice géorgien, de l'Agence d'échange des données en tant qu'entité centrale responsable de l'élaboration et de l'application des politiques et normes relatives à l'information et à la cybersécurité, et chargée principalement :

- D’adopter et d’appliquer les normes et directives de sécurité informatique relatives au secteur public et aux infrastructures essentielles;
- De s’acquitter de son mandat en matière de cybersécurité en créant une équipe nationale d’intervention informatique d’urgence;
- D’assurer des services de conseil en information et cybersécurité, d’effectuer des évaluations dans le domaine de la sécurité de l’information et d’assurer des services de cybersécurité;
- De mener des activités de sensibilisation en matière d’information et de cybersécurité.

Le cadre juridique et réglementaire de la Géorgie en ce qui concerne la sécurité de l’information se compose de la loi sur la sécurité de l’information et des textes complémentaires adoptés entre 2011 et 2012. Les principaux concepts utilisés dans la législation géorgienne sur les politiques en matière de sécurité de l’information proviennent de la série 27000 des normes de l’Organisation internationale de normalisation. La loi met l’accent sur certains droits et obligations afférents aux infrastructures essentielles dans le cadre de l’application des politiques de sécurité de l’information et établit des mécanismes de coopération avec des équipes nationales d’intervention informatique d’urgence.

La Géorgie a pris des mesures importantes pour renforcer la coopération internationale et partager les connaissances accumulées avec ses partenaires. Un exemple parlant est le nombre d’accords de coopération bilatéraux et de mémorandums d’entente entre l’Agence d’échange des données et les états-majors de pays de l’Union européenne (Autriche, Estonie, Pologne, etc.) et des pays voisins (Azerbaïdjan, Arménie, République de Moldova, Turquie, etc.).

La Géorgie reconnaît l’importance accrue des mécanismes de coopération régionale et internationale pour faire face aux problèmes qui se posent en matière de sécurité de l’information. Dans cette perspective, davantage d’efforts devraient être déployés pour accroître le nombre d’événements internationaux consacrés à ces questions de haute importance, pour augmenter la confiance des principales parties prenantes et pour continuer à travailler sur les doctrines stratégiques et sur les concepts juridiques avec la participation de la communauté internationale.

Panama

[Original : espagnol]
[3 juin 2015]

Les technologies de l’information et des communications connaissent une expansion rapide de nos jours. En conséquence, les technologies et les communications deviennent de plus en plus accessibles pour les Panaméens dans leur vie de tous les jours.

C’est un fait : aujourd’hui, nos vies sont liées à cette évolution en matière de communication et de traitement des informations.

Le Gouvernement panaméen a agi conformément à cette tendance et l’a adaptée aux besoins particuliers du service de sécurité. C’est la raison pour laquelle

il a procédé à des améliorations techniques afin d'assurer une connectabilité plus efficace et sûre.

Dans le cadre de ces améliorations, le Gouvernement panaméen met progressivement au point un plan de mise en œuvre des communications, qui comprend des éléments concernant les réseaux, la sécurité et la téléphonie. Les fabricants ont confirmé que ces éléments étaient conformes aux normes internationales.

Le Gouvernement panaméen protège l'intégrité de ses informations dans le domaine de l'Internet, des données et de la téléphonie grâce à des infrastructures telles que des plateformes pare-feu internes et grâce à une connexion avec le réseau multiservices national.

Le Gouvernement utilise des pare-feu pour sécuriser les données, afin de garantir la confidentialité et la protection des informations.

Nous estimons que, comme de plus en plus de solutions optimales en matière de télécommunications sont adaptées aux besoins de sécurité des services de sécurité, ces organismes auront accès à des outils pouvant favoriser l'harmonie dans le domaine de l'information sur la base de mesures à la fois actives et préventives. Les organismes de sécurité devraient tirer profit de cette évolution technologique, étant donné que nous avons pour mission de protéger la société aux niveaux local et international.

Pays-Bas

[Original : anglais]
[29 mai 2015]

La communauté internationale a un intérêt commun à assurer que le cyberespace reste libre, sûr et ouvert à tous et elle en a la responsabilité. Les Pays-Bas estiment que l'acceptation par plus grand nombre et l'application d'un ensemble de normes de comportement responsable des États serviraient la sécurité. Un travail appréciable a déjà été effectué par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Toutefois, un travail plus approfondi pourrait être effectué et des mesures concrètes pourraient être prises dans les domaines suivants :

- Aider les États à mieux comprendre la manière dont le droit international et les normes liées aux règles de conduite des États s'appliquent au cyberespace, en particulier le cadre juridique international en vigueur pour les cyberopérations qui ne donnent pas lieu à une attaque armée;
- Définir des normes ou de nouvelles mesures d'autolimitation ou d'entraide, en particulier mettre en place une protection normative spéciale pour certains systèmes et réseaux, notamment les infrastructures essentielles qui fournissent les principaux services civils, les structures d'intervention en cas d'incident civil et certaines composantes essentielles de l'Internet mondial;
- Renforcer les capacités juridiques, diplomatiques et politiques et l'échange de pratiques optimales dans le domaine de la sécurité et de la paix internationales en matière de cyberespace. Le Forum international sur le cyberespace, qui a

été lancé à La Haye à l'occasion de la quatrième Conférence internationale sur le cyberespace, peut jouer un rôle de premier plan à cet égard.

Alors qu'Internet devient un outil stratégique pour nous tous, un débat international sur ces questions s'avère nécessaire. Les Pays-Bas continueront à aider activement à promouvoir ce dialogue.

On trouvera le texte intégral de la réponse des Pays-Bas à l'adresse suivante : www.un.org/disarmament/topics/informationsecurity/.

Pérou

[Original : espagnol]
[30 juin 2015]

Évaluation générale des problèmes de sécurité de l'information par la Direction de l'informatique

- Le réseau de gestion des données de la Police nationale péruvienne permet de contrôler ses différents systèmes au moyen de politiques de sécurité appliquées à plusieurs niveaux de sa structure organique et fonctionnelle.
- En ce qui concerne la sécurité de l'information, le réseau de gestion des données a été externalisé vers le service de sécurité public géré par un centre des opérations de sécurité.
- Des travaux d'ingénierie sur le rôle et l'identité sont prévus; ils permettront un contrôle exceptionnel des accès des utilisateurs, en assurant la traçabilité et en fournissant des outils de vérification.

Efforts engagés au niveau national pour renforcer la sécurité informatique

Mesures préventives

- Nomination d'administrateurs de réseau
- Formation du personnel à l'informatique
- Octroi de licences de logiciels pour les serveurs du centre de données de la Police nationale
- Mise en place de dispositif de stockage en nuage privé
- Sauvegarde d'informations
- Mise en place d'un système électrique de secours (alimentation électrique constante)
- Mise à jour des tableaux de distribution électrique et des raccords électriques
- Externalisation du périmètre de sécurité (externe) en cas d'attaque ou de déni de service

Contenu des principes mentionnés dans le titre de la résolution

- Mise à jour de la plateforme informatique de la Police nationale et des systèmes d'information de la police, qui ont pour objet de regrouper les moyens informatiques aidant véritablement à améliorer la sécurité publique

nationale et de contribuer à la sécurité internationale par l'offre de services garantissant l'interopérabilité entre pays

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

- Normalisation des moyens de communication, y compris en ce qui concerne le type de matériel et les protocoles de communication
- Normalisation d'une plateforme technologique toujours disponible et consacrée à l'interopérabilité entre pays travaillant à la sécurité internationale
- Normalisation des mécanismes de sécurité informatique
- Dans le cadre du concept « domaine de l'information », définition de facteurs de risque réels dans chaque pays travaillant à la sécurité internationale et possibilité de fixer des objectifs communs en ce qui concerne ce qui doit être combattu ou maîtrisé avec la création de mécanismes d'information automatisés. Par exemple, dans le cas du Pérou, des questions telles que le trafic de drogue, le terrorisme, la criminalité organisée, la contrebande, le blanchiment d'argent et le trafic d'êtres humains seraient incluses.

Portugal

[Original : anglais]
[24 avril 2015]

Dans sa résolution 69/28 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 elle a notamment constaté que les innovations dans ces domaines pouvaient se prêter à des applications civiles aussi bien que militaires. Alors que les progrès dans les domaines de l'information et des télécommunications semblent offrir de très vastes perspectives pour le progrès de la civilisation, la multiplication des possibilités de coopération pour le bien commun de tous les États, le renforcement du potentiel créatif de l'humanité et l'amélioration de la circulation de l'information dans la communauté mondiale, nous estimons 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 la même résolution, l'Assemblée générale a invité les États Membres à collaborer dans quatre domaines, en tenant compte 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 (A/68/98), à savoir :

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

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

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

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

Le rapport du Groupe d'experts gouvernementaux contient des recommandations dans les domaines suivants : normes, règles et principes de comportement responsable des États; mesures visant à instaurer la confiance et l'échange d'informations; et mesures de renforcement des capacités.

Partant de ces recommandations, on peut décrire la situation du Portugal 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.

Nous devons redoubler d'efforts pour faire appliquer la législation en matière de sécurité et d'intégrité des réseaux, en adoptant des méthodes en matière de risque qui nécessitent l'adoption de mesures de sécurité adaptées sur les plans technique et organisationnel et imposent de signaler les violations de la sécurité ou les atteintes à l'intégrité qui ont des conséquences non négligeables pour le fonctionnement des services.

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

Sur le plan international, il est important de renforcer les échanges d'informations et d'effectuer des exercices de formation sur le terrain dans les zones frontalières.

Mesures de renforcement de la confiance et échange d'informations

Compte tenu de la mondialisation, il est indispensable d'encourager les échanges d'informations parmi toutes les parties prenantes (publiques et privées).

Les efforts déployés à l'échelon national ont porté essentiellement sur l'exécution d'exercices conjoints auxquels participent des entités publiques et privées, la promotion de la normalisation sur le plan technique et l'organisation de conférences et 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, mais 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, y compris la sécurité, auprès de toutes les parties prenantes principales.

Qatar

Original : arabe]
[24 juin 2015]

L'État du Qatar continue de surveiller les menaces réelles et potentielles dans le domaine de la sécurité de l'information. Il a défini des stratégies pour faire face à ces menaces tout en préservant la libre circulation de l'information. L'État du Qatar est d'avis que la sécurité de l'information est d'une importance cruciale pour la sécurité nationale et mondiale. Dans le but d'assurer la sécurité de l'information, l'État du Qatar a pris une série de mesures visant à mettre à jour les technologies pertinentes et à améliorer la législation, la réglementation et leur application. Il s'efforce également de coordonner les actions et de coopérer sur les questions pertinentes aux niveaux régional et international, à condition que le droit interne l'autorise.

L'État du Qatar estime que la communauté internationale peut contribuer à la sécurité de l'information en continuant à œuvrer en faveur d'un instrument international contraignant propre à garantir. Un tel instrument devrait permettre d'élaborer des programmes protégés contre le piratage et d'assurer la cohérence des systèmes d'information.

République de Corée

[Original : anglais]
[11 juin 2015]

À l'heure actuelle, le cyberespace est un nouvel horizon offrant des possibilités infinies et des avantages économiques et sociaux sans précédent. Toutefois, étant donné que le cyberespace, par nature, est ouvert à tous, permet l'anonymat et ne connaît pas les frontières, les menaces cybernétiques sont en passe de devenir un obstacle de taille à la sécurité internationale.

La République de Corée a connu une série de cyberattaques, y compris les récentes attaques contre ses centrales nucléaires en 2014. Afin de réagir de manière plus efficace aux menaces cybernétiques, la République de Corée a présenté en mars 2015 des plans complets pour améliorer la cybersécurité et a créé le poste de secrétaire de la présidence pour la cybersécurité. La République de Corée est convaincue qu'il est important de se mettre d'accord sur un ensemble de normes internationales qui s'appliquent au cyberespace et d'appliquer des mesures de renforcement de la confiance et des capacités cybernétiques.

À cet égard, la République de Corée salue les résultats présentés dans le rapport de 2013 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui a reconnu qu'il était possible d'appliquer le droit international au comportement des États dans le cyberespace et elle compte sur de plus amples discussions sur la façon dont les principes convenus peuvent être appliqués au comportement des États dans le cyberespace. La République de Corée a accueilli le séminaire régional Asie-Pacifique sur le droit international et le comportement des États dans le cyberespace en 2014, en partenariat avec l'Institut des Nations Unies

pour la recherche sur le désarmement, une occasion pour les pays de la région de discuter des questions relatives à la cybersécurité.

Le Gouvernement de la République de Corée s'est également employé à renforcer la coopération bilatérale et trilatérale avec des pays clefs et il participe activement aux forums régionaux et internationaux sur les questions cybernétiques, tels que le Forum régional de l'Association des nations de l'Asie du Sud-Est et le Groupe d'experts gouvernementaux des Nations Unies. En tant qu'hôte de la Conférence de Séoul sur le cyberespace tenue en 2013, la République de Corée a coopéré étroitement avec les Pays-Bas pour préparer la Conférence internationale sur le cyberespace, organisée à La Haye en 2015, et le pays entend continuer à contribuer aux conférences de Londres appelées London Process Conferences.

On trouvera le texte intégral de la réponse de la République de Corée à l'adresse suivante : www.un.org/disarmament/topics/informationsecurity/.

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

[Original : anglais]
[29 mai 2015]

Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord se félicite de l'occasion qui lui est donnée de répondre à la résolution 69/28 de l'Assemblée générale intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », et il reprend, dans la présente réponse, les propos qu'il avait tenus dans celle qu'il avait faite en 2013 comme suite à la résolution 68/243. Afin de ne pas créer de confusion, étant donné les interprétations différentes de l'expression « sécurité informatique » dans ce contexte, le Royaume-Uni emploie de préférence le mot « cybersécurité » et des concepts qui y sont liés dans sa réponse.

Le Royaume-Uni est conscient que le cyberespace constitue un élément clef des principales infrastructures nationales et internationales et qu'il est le socle essentiel des activités économiques et sociales en ligne. Les menaces réelles et potentielles associées aux activités menées dans le cyberespace sont très préoccupantes. Notre réponse porte sur les stratégies nationales et internationales qui ont été et seront adoptées pour renforcer la sécurité et promouvoir la coopération dans ce domaine. Ces approches reposent sur la stratégie nationale pour la cybersécurité du Royaume-Uni, publiée en novembre 2011.

Le Royaume-Uni continue de jouer un rôle de premier plan dans le débat international sur la cybersécurité. Nous avons fourni des experts pour les quatre Groupes d'experts gouvernementaux chargés d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et nous considérons que le rapport consensuel du dernier groupe constitue un pas précieux vers la définition d'une vision commune en ce qui concerne les normes de comportement des États dans le cyberespace et qu'il affirme que le droit international s'applique au cyberespace. Nous attendons avec impatience le résultat des débats du groupe actuel en juin 2015. Le Royaume-Uni se félicite en outre de la poursuite des discussions concernant d'éventuelles futures mesures de renforcement de la confiance dans le cyberespace au sein de l'Organisation pour la sécurité et la coopération en Europe, qui prolongeraient celles

négociées avec succès en 2013 et salue les activités similaires menées dans d'autres organisations régionales.

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 et les aptitudes dans ce domaine. Le Royaume-Uni attend avec intérêt la poursuite des progrès dans tous ces domaines. Le Royaume-Uni se félicite de contribuer activement à la résolution de ces questions importantes et il aura à cœur de poursuivre sa participation au renforcement des capacités et de la coopération internationale en matière de cybersécurité.

On trouvera le texte intégral de la réponse du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord à l'adresse suivante : www.un.org/disarmament/topics/informationsecurity/.