Nations Unies A/71/172

Assemblée générale

Distr. générale
19 juillet 2016
Français
Original : anglais/arabe/espagnol/
français/russe

Soixante et onzième session
Point 94 de l'ordre du jour provisoire*

Progrès de l'informatique et des télécommunications et sécurité internationale

Rapport du Secrétaire général

Table des matières

* A/71/150.

16-12486X (F)

I. Introduction

1. Le 23 décembre 2015, l'Assemblée générale a adopté la résolution 70/237, intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale ». Au paragraphe 4 de cette résolution, l'Assemblée générale invite tous les États Membres à continuer de communiquer au Secrétaire général, en tenant compte des constatations et recommandations figurant dans le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de 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 3 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 15 février 2015, les invitant à communiquer des informations à ce sujet. Les réponses reçues au moment de la rédaction du présent rapport sont reproduites dans la section II ci-dessous. Si d'autres réponses sont reçues ultérieurement, elles seront publiées sous forme d'additifs au présent rapport. Le texte intégral de toutes les communications figure à l'adresse suivante :www.un.org/disarmament/topics/informationsecurity.

II. Réponses reçues des gouvernements

Albanie

[Original : anglais]

[15 avril 2016]

La principale priorité de l'Albanie dans le domaine de la sécurité et de la protection des informations classifiées est la signature de l'accord entre le Gouvernement de la République d'Albanie et l'Union européenne relatif aux procédures de sécurité en matière d'échange et de protection des informations classifiées. L'accord susvisé a été signé le 3 mars 2016 à Tirana et devrait être ratifié en temps voulu par l'Assemblée de la République d'Albanie.

Pour mettre en place et appliquer les mesures appropriées en Albanie, en vue de renforcer la sécurité informatique et de promouvoir la coopération internationale en la matière, il a été procédé à la révision des textes juridiques suivants:

- La décision n°188 du Conseil des ministres, en date du 4 mars 2015, relative à l'approbation des règlements sur la sécurité du personnel ;

- La décision n°189 du Conseil des ministres, en date du 4 mars 2015, relative à la sécurité physique des informations classifiées portant la mention « Information de l'OTAN, Secret d'État » ;
- La décision n°190 du Conseil des ministres, en date du 4 mars 2015, portant plusieurs modifications et ajouts à la décision n°81 du Conseil des ministres définissant les critères et les procédures de destruction des informations classifiées ;
- La décision n°701 du Conseil des ministres, en date du 22 octobre 2014, portant approbation des règles de sécurisation des informations classifiées du domaine industriel.

L'Albanie possède une réglementation juridique exhaustive sur la sécurité physique des informations classifiées. Les « domaines de sécurité » sont redéfinis et identifiés en tenant compte des différents niveaux de classification des informations.

Suite à l'adoption de la nouvelle décision en matière de sécurité du personnel, la coopération interinstitutionnelle et la supervision et l'inspection des institutions de l'État ont été renforcées. Les organismes d'État ont lancé un processus de révision des listes de tâches du personnel et de délivrance des certificats de sécurité adéquats selon les domaines de responsabilité.

Pour ce qui concerne la sécurité industrielle, l'Albanie a concentré ses efforts sur l'examen de la politique de cybersécurité, en révisant les procédures en usage au Conseil des ministres par la décision n°701 du 22 octobre 2014.

Une autre étape importante à souligner est l'élaboration d'une nouvelle loi sur le traitement des informations classifiées. Cette loi mettra à jour la règlementation selon des normes européennes élevées. La législation nationale dans ce domaine est révisée en tenant compte de l'Acquis de l'Union européenne et, notamment, de la décision 2013/488/EU du Conseil relative aux règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne.

Australie

[Original : anglais]

[31 mai 2016]

L'Australie se félicite de l'occasion qui lui est donnée, en réponse à l'appel contenu dans la résolution 70/237 de l'Assemblée générale, d'exprimer son opinion sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. La présente communication s'inspire des informations fournies par l'Australie en réponse à la résolution 68/243 de 2014 et à la résolution 65/41 de 2011.

La cybersécurité est intimement liée à l'innovation et à la sécurité nationale. Elle est le socle de l'innovation, de la croissance et de la prospérité. La cybersécurité offre aux gouvernements, aux opérateurs du secteur privé et à la communauté des perspectives mondiales dans lesquelles s’investir et desquelles tirer avantage.

La communauté mondiale doit garantir la cybersécurité. Toutes les parties, que ce soit les gouvernements, les entreprises ou les particuliers, doivent travailler ensemble pour construire un cyberespace fiable. Cela est nécessaire pour protéger les informations sensibles, mais aussi pour fournir un environnement propice à l'innovation, au développement de l'industrie technologique, et pour tirer pleinement parti de la nécessaire amélioration – à l'échelle mondiale – des solutions et des équipements de cybersécurité et des compétences des professionnels du secteur.

L'Australie est consciente qu'une cybersécurité sans faille constitue un facteur crucial pour la croissance et la prospérité de l'économie mondiale. En 2015, l'Australie a révisé sa politique en matière de cybersécurité et a lancé sa nouvelle stratégie de cybersécurité le 21 avril 2016.

L'Australie estime que l'une des tâches prioritaires de la communauté internationale consiste à définir la manière dont le droit international devra s'appliquer au comportement des États dans le cyberespace, en particulier dans les situations de paix. Il faudra déployer des efforts supplémentaires pour se mettre d'accord sur l'application de concepts fondamentaux tels que la souveraineté et la juridiction dans le cyberespace, en tenant compte de notre intérêt commun de préserver le caractère mondial de l'Internet. Il est possible d'améliorer davantage les normes volontaires énoncées dans le rapport de 2015 du Groupe d'experts gouvernementaux relatives à la protection des infrastructures critiques, aux équipes d'intervention en cas d'urgence informatique, à la responsabilité des États en matière d'assistance, à la coopération en matière de cybercriminalité et à la prévention de la prolifération d'outils et de techniques informatiques malveillants. Il importe de faire avancer les travaux sur les mesures de confiance et de passer à la phase suivante, de la promotion de la transparence à la mise en œuvre des mesures de coopération.

Canada

[Original : anglais]

[27 mai 2016]

Concernant le cyberespace, le Canada estime que :

- Un cyberespace libre, ouvert et sécurisé est essentiel à la sécurité mondiale, à la prospérité économique et à la promotion des droits de l'homme, de la démocratie et de l'inclusion ;
- Toute approche de lutte contre les cybermenaces doit aller de pair avec le respect des droits de l'homme et des libertés fondamentales ;
- Le droit international actuel s'applique à l'utilisation par les États des technologies de l'information et des communications ;
- Promouvoir les normes applicables en temps de paix contribue à créer un environnement propice au comportement responsable qui guide les actions des États, favorise le partenariat et renforce la stabilité du cyberespace ;
- Les mesures de confiance réduisent les tensions et le risque de conflits armés ;

Au plan national, depuis la publication en 2010 de sa Stratégie de cybersécurité, le gouvernement canadien a poursuivi ses efforts de sécurisation des cybersystèmes canadiens et de protection de ses citoyens dans le cyberespace. Le Canada a, par ailleurs, lancé une campagne de sensibilisation intitulée « Pensez cybersécurité ». Le gouvernement s'est engagé récemment à revoir les mesures actuelles de protection des Canadiens et des infrastructures sensibles des cybermenaces.

Au plan international, le Canada contribue de différentes façons aux questions relatives au cyberespace, ainsi :

- Le Canada continuera à promouvoir la mise au point de normes applicables en temps de paix relatives au comportement des États dans le cyberespace, notamment les résultats du Groupe d'experts gouvernementaux de 2012-2013 et 2014-2015. Le Canada a été sélectionné pour participer au Groupe d'experts en 2015-2016 ;
- Le Canada a ratifié la Convention de Budapest en juillet 2015 et encourage les pays à la ratifier ou à y adhérer, ou à s'en inspirer pour appliquer leurs propres législations en matière de cybercriminalité ;
- Depuis 2007, le Canada s'est engagé à apporter une contribution au montant de 8,25 millions de dollars pour des projets de renforcement des capacités en matière de cybersécurité dans les Amériques et en Asie du Sud-Est ;
- Le Canada est membre fondateur du Forum mondial sur la Cyber Expertise ;
- Le Canada collabore avec les États-Unis pour harmoniser nos actions de sensibilisation du public à la cybersécurité par le biais de la campagne « *Stop. Think. Connect* ».
- Le Canada collabore également avec les États-Unis pour mettre en œuvre le Plan d'action Canada-États-Unis sur la cybersécurité, qui vise à renforcer la résilience de la cyberinfrastructure ;
- Le Canada participe à l'élaboration de mesures de confiance dans divers forums, 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.
- Le Canada appuie les efforts que déploie l'Organisation du Traité de l'Atlantique Nord (OTAN) pour renforcer la cybersécurité de l'Alliance et celle de ses alliés. Le Canada a apporté un million de dollars au Centre d'excellence pour la cyberdéfense de l'OTAN ;
- Le Canada appuie l'utilisation des technologies de l'information et des communications (TIC) comme outils de développement, notamment pour aider les organisations de la société civile à offrir des services essentiels tels que l'aide d'urgence dans les situations de conflit;

Le Centre de recherches pour le développement international du Canada a contribué au progrès du développement mondial en mettant des technologies de l'information et des communications au profit de la recherche sur le développement et du renforcement des capacités.

Colombie

[Original : espagnol]
[13 juin 2016]

Grâce à son Plan « Vive Digital » (2010-2014) et au nouveau Plan « Vive Digital – para la gente » (2014-2018), la Colombie a connu une révolution numérique qui a permis de passer, en cinq années seulement, de 2,2 millions de connexions Internet à plus de 12,2 millions. Elle sera le premier pays d'Amérique latine à avoir un accès Internet haut débit dans toutes ses municipalités. Au cours de la même période, plus de deux millions de terminaux ont été remis à des établissements scolaires. Soixante-quatorze pour cent des micro-entreprises et des petites et moyennes entreprises bénéficient aujourd'hui d'une connexion Internet, contre 7 % en 2010. Nous avons enregistré également un taux de 90 % d'augmentation de la pénétration d'Internet dans les ménages et nous avons ramené l'Internet dans les campagnes et dans les endroits les plus reculés. En effet, 7 621 centres « Vive Digital » ont été ouverts dans les zones rurales de plus de 100 habitants. Parmi d'autres réalisations, la Colombie est le pays d'Amérique latine qui compte le plus d'entrepreneurs numériques; on en recense plus de 100 000.

Le Gouvernement colombien reconnaît qu'il n'est pas possible d'optimiser l'utilisation des technologies de l'information et des communications et d'en tirer le meilleur parti si les citoyens ou les entreprises s'en méfient, c'est-à-dire, si l'environnement numérique ne leur inspire pas un sentiment de sécurité. Les incidents qui surviennent de plus en plus fréquemment conditionnent cette perception.

a) Efforts engagés au niveau national pour renforcer la sécurité informatique et promouvoir les activités de coopération internationale dans ce domaine :

La Colombie vient de lancer une politique nationale de sécurité numérique, présentée dans le document CONPES 3854 de 2016. Cette politique vise à garantir que les pouvoirs publics, les organisations publiques et privées, les forces de l'ordre, le milieu universitaire et les Colombiens, en général, disposent d'un environnement numérique fiable et sûr qui maximise les bienfaits économiques et sociaux, favorisant ainsi la compétitivité et la productivité dans tous les secteurs de l'économie. Fruit d'un processus associant plusieurs parties prenantes, elle constitue l'une des premières politiques nationales au monde (elle est la première dans la région) à suivre la recommandation de l'Organisation de coopération et de développement économiques sur la gestion du risque de sécurité numérique, adoptée en septembre 2015.

Cette politique préconise, en premier lieu, la mise en place d'un cadre institutionnel clair pour la sécurité numérique. Pour ce faire, des instances de coordination et d'orientation chargées de la sécurité numérique seront créées au plus haut niveau de l'État et des services de liaison sectorielle seront mis en place dans l'ensemble des structures du pouvoir exécutif à l'échelle nationale. En deuxième lieu, il faudra instaurer des conditions propices pour permettre aux différentes parties prenantes de gérer le risque de sécurité numérique dans leurs activités socioéconomiques et pour inspirer la confiance quant à l'utilisation du numérique grâce à des mécanismes de participation active et permanente, à un cadre juridique et réglementaire en la matière et à une formation destinée à inculquer des comportements responsables dans l'environnement numérique. En troisième lieu, il

s'agira de renforcer la défense et la sécurité nationales au sein de l'environnement numérique, tant sur le plan national que transnational, en adoptant une approche de gestion des risques. Enfin et surtout, la politique prévoit de créer des mécanismes permanents pour promouvoir la coopération, la collaboration et l'assistance en matière de sécurité numérique à l'échelle nationale et internationale, dans le cadre d'une approche stratégique.

b) Principes visés au paragraphe 3 de la résolution 70/237 :

En tant que membre du Groupe d'experts gouvernementaux (2014-2015), récemment créé, la Colombie partage sans réserve le point de vue selon lequel il est nécessaire de poursuivre la réflexion sur les principes relatifs à la sécurité informatique et aux systèmes mondiaux de télécommunication et les aspects liés à l'applicabilité du droit international dans le cyberespace.

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

Dans l'esprit de ce qui précède, nous souscrivons pleinement aux importantes recommandations émises par consensus par le Groupe d'experts gouvernementaux. Elles portent notamment sur l'adoption, à titre facultatif, de mesures et de bonnes pratiques, ainsi que sur le renforcement des capacités et la coopération des États pour promouvoir l'utilisation pacifique des technologies de l'information et des communications, de sorte qu'elles demeurent des outils de développement économique et social pour les pays, en particulier pour les pays les moins avancés dans le domaine technologique.

Cuba

[Original : espagnol]
[vendredi 6 mai 2016]

Cuba partage la préoccupation exprimée dans la résolution 70/237 selon laquelle les technologies et les moyens informatiques 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 civil et militaire.

Cette résolution insiste avec pertinence sur la nécessité de prévenir l'utilisation des moyens et des technologies informatiques à des fins criminelles ou terroristes.

A cet égard, Cuba réitère son inquiétude quant à l'utilisation clandestine et illégale, par des individus, des organisations et des États, des systèmes informatiques d'autres nations pour attaquer des pays tiers, ce qui risque de provoquer des conflits internationaux.

Seule la coopération étroite entre tous les États pourra prévenir ces menaces et les juguler et éviter que le cyberespace se transforme en théâtre d'opérations militaires.

L'usage des télécommunications dans le but déclaré ou inavoué de porter atteinte à l'ordre juridique et politique des États constitue une atteinte aux normes

internationales en la matière et peut créer des tensions et des situations susceptibles de porter atteinte à la paix et à la sécurité internationales.

Au deuxième Sommet des chefs d'État et de gouvernement des États Membres 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 la région d'Amérique latine et des Caraïbes était une zone de paix afin, entre autres, de favoriser des relations d'amitié et de coopération entre eux et avec d'autres nations, indépendamment des différences 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 quatrième Sommet des chefs d'État et de gouvernement des États Membres de la Communauté des États d'Amérique latine et des Caraïbes, qui s'est tenu à Quito, en janvier 2016, les États Membres ont souligné de nouveau que les technologies de l'information et des communications, y compris Internet, étaient des outils non négligeables pouvant encourager la paix et promouvoir le bien-être humain, le développement, les connaissances, l'inclusion sociale et la croissance économique. De même, l'utilisation pacifique des technologies de l'information et des communications, conformément aux buts et principes énoncés dans la Charte des Nations Unies et au droit international, a été réaffirmée, et les États ont souligné que ces technologies ne devraient jamais être utilisées pour nuire à la société ou créer des situations susceptibles de provoquer des conflits entre États.

Ces efforts continuent néanmoins d'être menacés par toutes les émissions de radiodiffusion et de télévision que le Gouvernement des États-Unis transmet contre Cuba, en violation des buts et des principes consacrés dans la Charte des Nations Unies et dans divers règlements de l'Union internationale des télécommunications, et en violation également de la souveraineté de Cuba.

Par le biais d'émissions de radio et de télévision illégales, l'espace radiophonique de Cuba est violé de manière régulière. Des programmes spécialement conçus pour appeler au renversement de l'ordre constitutionnel établi par le peuple cubain ont été diffusés. À titre d'exemple, rien qu'au cours des trois premiers mois de 2016, quelques 1 880 heures d'émissions hebdomadaires anticubaines ont été diffusées illégalement, utilisant 23 fréquences.

Cuba espère voir ces politiques d'agression cesser immédiatement; elles sont d'ailleurs incompatibles avec la décision des Gouvernements cubain et américain d'établir des liens fondés sur le respect mutuel et la coopération, lors du rétablissement des relations diplomatiques entre les deux pays.

Cuba espère également que l'embargo économique, commercial et financier, à l'origine des graves souffrances du peuple cubain, sera levé. L'embargo a eu des conséquences préjudiciables dans le domaine de l'information et des communications et dans d'autres sphères de la vie quotidienne des Cubains.

La coopération internationale est essentielle pour faire face aux dangers liés à l'utilisation abusive des technologies de l'information et des communications. L'Union internationale des télécommunications a un rôle important à jouer dans les débats intergouvernementaux sur les problématiques de cybersécurité.

Cuba a appuyé la résolution 70/237 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]
[mardi 26 avril 2016]

Les forces armées d'El Salvador ont renforcé le matériel informatique de sécurité des périmètres et ont mis en œuvre des politiques de sécurité pour régir l'accès aux ressources du réseau informatique (mots de passe des utilisateurs modifiés régulièrement, accès restreint aux ports USB et aux lecteurs de DVD et de CD et accès bloqué au disque C du matériel).

Espagne

[Original : espagnol]
[26 mai 2016]

L'Espagne considère que les technologies de l'information et des communications ouvrent des possibilités immenses et ne cessent de gagner en importance pour la communauté internationale. Il existe toutefois des tendances préoccupantes qui présentent des risques pour la paix et la sécurité internationales. Il est indispensable que les États coopèrent efficacement pour prévenir les pratiques nocives dans le cyberespace et ils ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre, à l'aide de ces technologies, des actes punis à l'échelle internationale.

En juillet 2015, le Conseil national de la cybersécurité a adopté neuf plans découlant du Plan national de cybersécurité et définissant les différentes lignes d'action prévues dans la stratégie nationale de cybersécurité de 2013.

L'Espagne participe activement à toutes les initiatives stratégiques ayant des incidences sur la cybersécurité au sein de l'Union européenne, de l'Organisation pour la sécurité et la coopération en Europe, de l'Organisation du Traité de l'Atlantique Nord, du Conseil de l'Europe et de l'Organisation de coopération et de développement économiques.

En 2015, l'Espagne a adhéré à la Freedom Online Coalition et au Global Forum on Cyber Expertise.

L'Espagne appuie le document final de la réunion de haut niveau de l'Assemblée générale sur l'examen d'ensemble de la mise en œuvre des textes issus du Sommet mondial sur la société de l'information, adopté en décembre 2015.

L'essor de la connectabilité, de l'innovation et de l'accès dans le domaine des technologies numériques a été essentiel aux progrès accomplis dans la réalisation des objectifs du Millénaire pour le développement. L'Espagne estime qu'il est nécessaire que les mesures visant à donner suite aux textes issus du Sommet mondial sur la société de l'information soient harmonisées avec le Programme de développement durable à l'horizon 2030, car l'accès à ces technologies est devenu un indicateur de développement et une finalité en soi.

L'Espagne soutient le processus devant aboutir à un consensus international en matière de cybersécurité et estime que les États doivent continuer à étudier plus en détail l'interprétation et l'applicabilité des principes et des normes du droit international dans le cyberespace, notamment ceux portant sur le recours à la menace ou à l'emploi de la force, le droit humanitaire et la protection des droits de l'homme et des libertés fondamentales.

L'Espagne appuie les aspirations de la communauté internationale à l'utilisation pacifique des technologies de l'information et des communications pour le bien commun de l'humanité. Elle considère que la Charte s'applique dans son intégralité et note que les États ont le droit fondamental de prendre des mesures conformes au droit international pour réagir de manière prompte, légitime et à la mesure des menaces ou des agressions susceptibles de nuire à la sécurité nationale.

Finlande

[Original : anglais]
[31 mai 2016]

La Finlande se réjouit de l'occasion qui lui est donnée de fournir des informations relatives à la résolution 70/237 de l'Assemblée générale. Les actions suivantes ont été entreprises au niveau national :

a) La Stratégie nationale de cybersécurité de la Finlande (2013) et son programme de mise en œuvre (2014) définissent les lignes directrices et les principales mesures de renforcement de la cybersécurité et de la résilience. Le Programme de mise en œuvre est mis à jour par le biais d'un processus de consultation multipartite et devrait être finalisé en 2016.

b) Depuis l'adoption de la Stratégie nationale de cybersécurité, la Finlande a créé un centre national de cybersécurité et un centre de prévention de la cybercriminalité et a désigné un ambassadeur chargé des questions de sécurité informatique. La Stratégie nationale de sécurité informatique a été adoptée en février 2016.

c) Dans le cadre de sa coopération au développement, la Finlande appuie divers projets de développement des technologies de l'information et des communications (TIC) et de renforcement des cybercapacités. La Finlande est membre fondateur du Forum mondial sur la Cyber Expertise. Elle a adhéré à l'Initiative Global Connect menée par les États-Unis, dont l'objectif est d'aider 1,5 milliard de personnes à se connecter à l'Internet d'ici 2020. Elle envisage de rejoindre le nouveau Fonds d'affectation spéciale de la Banque mondiale pour le partenariat pour le développement numérique. La Finlande appuie la gouvernance d'Internet selon un modèle multipartite.

d) La Finlande participe activement à un dialogue international sur les questions liées à l'Internet dans les forums multilatéraux et régionaux et dans ses contacts bilatéraux. Au sein de l'Organisation pour la sécurité et la coopération en Europe (OSCE), la Finlande participe au renforcement de la confiance, de la sécurité et de la stabilité dans le cyberespace et met en œuvre les mesures convenues pour le renforcement de la confiance et de la sécurité dans le cyberespace.

e) La Finlande a approuvé le rapport de 2015 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. La Finlande a participé activement aux discussions sur le droit international et le cyberespace, par exemple lors des consultations sur la version 2.0 du Manuel de Tallinn et les ateliers de l'Institut des Nations Unies pour la recherche sur le désarmement. La Finlande a rejoint la Freedom Online Coalition en 2012 et contribue au Digital Defenders Partnership.

f) La Finlande a ratifié la Convention de Budapest en 2007. Le nouveau Plan stratégique de la police, portant sur les ressources nécessaires à la prévention de la cybercriminalité et au développement du savoir-faire en matière de cybersécurité, a été lancé en 2015. D'autre part, un plan global de prévention de la cybercriminalité a été adopté.

Domaines prioritaires où la communauté internationale devrait déployer davantage d'efforts :

a) La Finlande attache beaucoup d'importance aux travaux du nouveau groupe d'experts gouvernementaux et se dit prête à contribuer à son succès, notamment pour établir des normes de comportement responsable des États dans le cyberespace en mettant un accent particulier sur les activités en temps de paix ;

b) Adopter et mettre en œuvre des mesures de confiance à l'échelon régional dans le cadre de l'OSCE ;

c) Continuer à renforcer les cybercapacités en vue d'améliorer la résilience et la sécurité dans le cyberespace ;

d) La Finlande continuera à soutenir et à encourager le dialogue multipartite. Le renforcement des partenariats public-privé à l'échelon national et international demeure prioritaire.

Inde

[Original : anglais]
[9 juin 2016]

Les technologies de l'information facilitent la croissance économique et la connectivité sociale, mais elles donnent lieu à de graves problèmes qui doivent traités. La croissance dans le secteur des technologies de l'information et des communications (TIC) s'accompagne d'une augmentation des cybermenaces telles que les cyberattaques, la cybercriminalité, le cyberterrorisme, l'espionnage et le blanchiment d'argent. Les faits montrent que des groupes terroristes (par exemple l'EIIL) utilisent l'Internet et les plates-formes des médias sociaux pour leurs activités néfastes, notamment le recrutement, la collecte de fonds, la propagande et la radicalisation. L'usage abusif des médias sociaux est une préoccupation majeure. Ces moyens ouvrent la voie à une connectivité impressionnante, mais ils peuvent également être utilisés à mauvais escient pour exacerber les dissensions ethniques et sociales.

Il importe à la communauté internationale de dégager une interprétation commune du comportement des États dans le cyberespace et d'adopter les mesures de confiance et de renforcement des capacités recommandées dans le rapport de

2015 du Groupe d'experts gouvernementaux. La question de la gouvernance de l'Internet ne devrait pas être noyée dans des débats sémantiques antagoniques. Diverses parties prenantes interviennent dans leurs domaines respectifs, mais les gouvernements ont un rôle primordial à jouer dans les questions de cybersécurité relatives à la sécurité nationale. Il est nécessaire de mettre en place des mécanismes appropriés pour le partage des informations relatives aux cybermenaces, à la cybercriminalité et au cyberterrorisme. Il importe également d'instaurer une coopération en temps réel entre les organismes gouvernementaux de lutte contre la cybercriminalité. En outre, la question de la cyberguerre, des cyberdoctrines et de leur impact sur la sécurité internationale doit être discutée dans tous les forums internationaux. Certes, les règles de comportement responsable des États dans le cyberespace ne sont pas encore convenues, mais il est possible de s'entendre sur une conception commune des mesures de confiance, telles qu'énoncées dans le rapport de 2015 du Groupe d'experts gouvernementaux, afin de renforcer les capacités dans le domaine de la cybersécurité. À cet égard, le cadre élaboré par le Forum mondial sur la Cyber Expertise propose des orientations utiles.

L'Inde est un acteur important dans l'utilisation des TIC. Elle appuie le partenariat multipartite dans la gouvernance de l'Internet et participe activement aux divers forums internationaux, notamment le Groupe d'experts gouvernementaux, le Processus de consultation ouvert sur l'examen global de la mise en œuvre des résultats du Sommet mondial sur la société de l'information, ainsi que la Société pour l'attribution des noms de domaine et des numéros sur Internet. En collaboration avec toutes les parties prenantes, l'Inde a adopté une approche intégrée comprenant une série de mesures politiques, juridiques, techniques et administratives pour répondre aux préoccupations relatives à la cybersécurité et promouvoir la coopération internationale dans ce domaine. Son cadre juridique est en harmonie avec d'autres cadres juridiques similaires de par le monde. La politique nationale de la cybersécurité (2013) a été mise en place afin de construire un cyberespace sécurisé et résilient pour les citoyens, les entreprises et le gouvernement. Elle accorde une importance particulière au renforcement des capacités, au développement des compétences et aux partenariats public-privé dans le domaine de la cybersécurité.

Japon

[Original : anglais]
[27 mai 2016]

Appréciation générale des questions qui se posent en matière de sécurité informatique

Le Japon estime que le cyberespace doit être un espace où la liberté est assurée sans restrictions inutiles et où tous les acteurs qui souhaitent y accéder ne doivent pas se voir refuser cet accès ou en être exclus sans motif légitime. Notre action est conforme aux cinq principes suivants : la libre circulation de l'information, la primauté du droit, la transparence, l'autonomie et l'approche multipartite.

Efforts déployés au niveau national pour renforcer la sécurité informatique et promouvoir la coopération internationale dans ce domaine

1. Efforts déployés au niveau national pour renforcer la sécurité informatique

Sur la base de sa stratégie de cybersécurité publiée en septembre 2015, le Japon déploie des efforts pour renforcer la sécurité informatique.

2. Efforts déployés au niveau national pour promouvoir la coopération internationale

Les mesures prises par le Japon reposent sur les trois piliers suivants : 1) la primauté du droit dans le cyberespace ; 2) les mesures de confiance ; et 3) le renforcement des capacités. En ce qui concerne 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 pour élaborer des normes, non contraignantes et volontaires, de comportement responsable des États. En ce qui concerne les mesures de confiance, 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 (ASEAN). En matière de renforcement des capacités, le Japon contribue activement à l'aide au développement des ressources humaines et à la coopération technique en se concentrant sur la région de l'ASEAN.

Principes visés au paragraphe 3 de la résolution

La confirmation de l'applicabilité du droit international et l'élaboration de normes non contraignantes et volontaires de comportement responsable des États dans le cyberespace sont essentiels à la stabilité et à la prévisibilité de la communauté internationale.

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

En ce qui concerne la primauté du droit, le Japon exhorte à la poursuite des délibérations sur l'élaboration de règles de droit international en temps de paix, sur le droit de légitime défense, sur le droit humanitaire international, ainsi que l'élaboration de normes volontaires lors des prochaines réunions du Groupe d'experts gouvernementaux. En ce qui concerne les mesures de confiance et le renforcement des capacités, il importe de promouvoir la mise en œuvre, par chaque État et chaque région, des recommandations contenues dans les rapports du Groupe d'experts gouvernementaux. Il est nécessaire d'examiner les moyens à mettre en œuvre pour une coopération concrète.

Jordanie

[Original : arabe]
[2 mai 2016]

Les technologies de l'information et des communications sont devenues essentielles dans notre vie quotidienne. Elles favorisent le développement et le progrès des communautés locales dans tous les domaines, notamment dans les sphères sociale, culturelle et économique, et ont de nombreuses implications sur l'interaction des individus au sein de leurs communautés et avec le reste du monde.

Les progrès remarquables et rapides des technologies de l'information et des communications les rendent vulnérables aux risques et aux défis. Ces risques et défis appellent des actions par des moyens technologiques et juridiques afin de

trouver des solutions pratiques et efficaces à l'effet de minimiser les risques et d'éviter les lourdes pertes qu'elles peuvent causer.

Les forces armées jordaniennes jouent un rôle actif et déterminant dans la promotion de la paix et de la sécurité aux niveaux national, régional et mondial à travers le développement et l'utilisation de la technologie pour garantir la sécurité de l'information et des télécommunications.

Ce rôle se manifeste dans les domaines suivants :

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 à travers tout le Royaume, y compris sur les frontalières, afin de renforcer la sécurité nationale et régionale ;

b) Coopération avec la communauté internationale pour le maintien de la sécurité internationale grâce à des systèmes de communication compatibles avec ceux utilisés par l'Organisation du Traité de l'Atlantique nord et les forces armées américaines et selon les 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 afin de renforcer la sécurité nationale et l'action des forces armées jordaniennes/l'armée arabe au service des opérations de maintien de la paix dans les zones de conflit à travers le monde ;

d) Formation et qualification de tous les utilisateurs et parties concernées pour pérenniser et entretenir tous les systèmes de communication, sans dépendre des fournisseurs, pour en rehausser la fiabilité et pouvoir 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 améliorer le niveau de coordination et de coopération en appui à la sécurité nationale, régionale et internationale ;

f) Participation active aux conférences internationales et mise en œuvre des décisions qui en découlent pour une plus grande complémentarité entre les armées amies, pour éviter les perturbations et les interférences entre les systèmes de communications utilisés par les pays voisins et de la région ; et assurer la coordination du contrôle et de la surveillance des frontières internationales.

Il convient de mettre l'accent sur la sensibilisation du citoyen à la cybersécurité et aux cybermenaces afin de minimiser les risques qui en découlent. Il convient également de sensibiliser davantage aux questions de sécurité pour faire face à tout type d'information d'une manière qui soit compatible avec l'utilisation de la technologie à bon escient.

Mesures de protection prises à l'échelle nationale pour protéger les réseaux informatiques de haute importance :

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

b) Utilisation de réseaux fermés (intranet) ;

c) Liaison avec les autres organismes de sécurité par le biais de dispositifs périphériques distincts ;

d) Application de mesures de 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 dans lesquels l'utilisateur interagit avec un écran contrôlé par le système selon l'autorisation d'accès et qui ne permet pas d'introduire des données ou d'avoir accès, par exemple au moyen d'un lecteur à mémoire flash.

f) La Jordanie a élaboré et promulgué une batterie de textes législatifs sur la cybersécurité, à savoir :

1. Promulgation d’une loi sur la cybercriminalité ;
2. Promulgation d’une loi sur les transactions électroniques ;
3. Elaboration d’un projet de loi sur la stratégie nationale de cybersécurité et de cyberprotection ;
4. Elaboration d’un projet de loi sur les politiques nationales en matière de cybersécurité et de cyberprotection ;
5. Adoption par le Conseil des ministres en 2012 de la Stratégie nationale en matière de cybersécurité et de cyberprotection ;

Actions proposées au niveau mondial :

a) Classifier les réseaux d'information et de communications selon leur importance ;

b) Mettre en œuvre des mesures de cybersécurité et de cyberprotection ;

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

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

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

f) Connecter les différents réseaux par des périphériques autarciques ;

g) Utiliser un Intranet privé dans certains réseaux et éviter d'utiliser le World Wide Web autant que possible ;

h) Renforcer l'intranet de l'Organisation des Nations Unies et l'autonomiser par rapport aux réseaux publics ; recourir aux mesures de sécurité et de protection nécessaires pour protéger ce réseau à l'aide de dispositifs de cryptage, de protection et de vérification d'accès ;

i) Renforcer la coopération entre équipes d'intervention informatique d'urgence en matière de suivi des infractions, de procédures de protection et de comblement des lacunes ;

j) Diffuser les procédures et les méthodes de traitement des violations de cybersécurité ;

Mettre l'accent sur l'utilisation des technologies de l'information et des communications pour réaliser le développement durable, en particulier dans les régions pauvres et reculées en :

a) Accélérant l'éradication de la pauvreté, notamment grâce aux services bancaires mobiles qui ont déjà apporté des avantages immédiats à des millions de personnes de par le monde qui n'ont pas d'expérience en matière de démarches bancaires ;

b) Atténuant les effets de la famine grâce aux technologies et aux moyens modernes qui fournissent les informations les plus importantes aux agriculteurs et leur permettent de prendre les décisions adéquates au sujet de leurs produits agricoles.

Recommandations **:**

a) Mettre sur pied des équipes internationales pour intervenir en cas d'incidents de sécurité informatique, aider à récupérer après de tels incidents et faire face aux catastrophes et crises informatiques ;

b) Intégrer un délégué de la Jordanie au Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui sera mis sur pied en 2016 ;

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

Liban

[Original : arabe]
[24 mai 2016]

Communication du ministère de la défense nationale du Liban :

Aujourd'hui, la cybersécurité concerne tous les domaines économiques, sociaux, politiques, militaires et humanitaires. Le cyberterrorisme est considéré comme le plus grand danger qui menace aussi bien les grandes puissances que les pays en développement.

La cyberguerre englobe les activités suivantes : création de sites web pour mobiliser les partisans, guerre psychologique, échange et diffusion d'informations à travers l'Internet, destruction de sites, de données et de systèmes informatiques, menaces et intimidation électroniques ;

Les attaques cyberterroristes sont en hausse dans tous les pays. Le Liban a été victime de plusieurs cyberattaques qui ont ciblé principalement le secteur bancaire, notamment par le virus "Gauss", ainsi que le secteur des télécommunications. La plupart des services électroniques sont attaqués en permanence.

Des efforts sont déployés au niveau national pour renforcer la cybersécurité et promouvoir la coopération internationale, à savoir :

- L'adoption, en 1999, de la loi n°140 relative à la protection du droit au secret des communications et la loi n° 75 sur la propriété intellectuelle, qui traitent en partie du piratage informatique ;
- La création, en 2006, du Bureau de lutte contre la cybercriminalité et de protection de la propriété intellectuelle auprès du Département des enquêtes criminelles et des opérations spéciales de la Direction générale des forces de sécurité intérieure ;

- La création, en 2007, de l'autorité de régulation des télécommunications, qui est devenue un membre actif du Partenariat multilatéral international de lutte contre les cybermenaces (IMPACT) ;
- La création en 2009, par le Commandement des forces armées, d'une section des preuves électroniques en matière criminelle auprès de la Direction du renseignement ;
- Le ministère de la Défense nationale s'emploie à mettre sur pied une équipe libanaise d'intervention en cas d'incidents informatiques en coopération avec les organismes nationaux et internationaux, et ce à travers la participation à toutes les initiatives et l'organisation de conférences et de stages de formation ;
- En 2012, le Conseil des ministres a décidé la création d'une commission nationale de sécurité qui encadre l'hébergement des sites Internet gouvernementaux, comprenant un représentant du Ministère de la défense nationale ;
- En 2013, le Conseil des ministres a mis sur pied une commission chargée d'étudier les menaces provenant des pylônes de télécommunications de l'ennemi israélien installés en face du territoire libanais ; cette commission est placée sous la présidence du Ministère de la défense nationale et est composée de représentants des ministères concernés ;
- En 2015, l'armée libanaise s'est dotée d'une section spécialisée dans la sécurité informatique.
- Actuellement, la Chambre des députés étudie un projet de loi sur les transactions électroniques.

Les mesures que la communauté internationale pourrait prendre pour renforcer la cybersécurité au niveau international sont les suivantes :

- L'application des résolutions adoptées par les Nations Unies et le Sommet mondial sur la société de l'information appelant à la diffusion de la cyberculture, à l'établissement d'un cadre de coopération avec les organismes internationaux spécialisés, garantissant l'échange des informations et le transfert des meilleures pratiques ;
- L'harmonisation des lois et des règlements nationaux de lutte contre la cybercriminalité avec le droit international pour prévenir l'émergence de paradis numériques ;
- La mise au point d'un système mondial capable de gérer les crises mondiales de cybersécurité et l'encouragement de l'adoption d'une législation internationale robuste et efficace pour appuyer les lois nationales des divers pays et les rendre plus aptes à faire face au caractère mondial et international de la cybercriminalité.

Pologne

[Original : anglais]
[18 juillet 2016]

1. Avis général

La cybersécurité est vitale pour le maintien de la croissance économique et le fonctionnement de la société civile. Les cyberattaques peuvent affecter non seulement le secteur privé et l'administration publique, mais aussi les équipements industriels automatisés d'infrastructures névralgiques.

Il est nécessaire d'assurer la cohérence des systèmes de sécurité de l'information et des télécommunications compte tenu de la nature des menaces et de la dépendance croissante des entreprises, de l'administration et de la société vis-à-vis des technologies de l'information. Toutes les parties prenantes, notamment les États, les opérateurs économiques et les organisations non gouvernementales, doivent participer et contribuer à la cybersécurité.

Le respect des normes et du droit internationaux est une condition nécessaire pour la préservation de la paix et de la sécurité entre les États dans le cyberespace.

L'amélioration des capacités nationales est essentielle pour renforcer la cybersécurité à l'échelle internationale.

Une confiance accrue dans le cyberespace aura un impact positif sur les relations entre les États dans d'autres domaines.

Il importe de protéger les droits de l'homme et les libertés fondamentales dans le monde virtuel et le monde réel. Le respect des libertés fondamentales sur Internet est essentiel pour la société démocratique, la croissance durable et la prospérité.

2. Initiatives nationales de renforcement de la cybersécurité et de la coopération internationale

Le système de cybersécurité polonais se base sur un réseau d'institutions. Il fait appel à la coopération des organismes civils et militaires, ainsi que des organismes chargés de la lutte contre la cybercriminalité.

Le Gouvernement polonais élabore actuellement une stratégie nationale de cybersécurité et prépare une législation nationale en matière de cybersécurité. Les principaux volets du système de cybersécurité polonais reposent sur les processus, les personnes et la technologie.

L'année dernière, la Pologne a accueilli plusieurs grands événements internationaux qui ont contribué à la promotion de la coopération internationale. Il s'agit de la Conférence SECURE 2015, du Forum européen sur la cybersécurité (www.cybersecforum.eu) et de la Conférence internationale sur la cybersécurité, la sécurité et la sûreté au-delà des frontières.

3. Mesures susceptibles de renforcer la cybersécurité à l'échelle mondiale

Il est nécessaire d'élaborer des mesures permettant de renforcer davantage la confiance dans le cyberespace qui devront être mises en œuvre au niveau mondial, régional et national.

La communauté internationale devrait encourager la création de capacités nationales en matière de cybersécurité.

Il importe d'approfondir la coopération bilatérale et régionale. La Plate-forme de cybersécurité de l'Europe centrale constitue un bon exemple de coopération

régionale. Elle regroupe la Pologne, la République tchèque, la Slovaquie, la Hongrie et l'Autriche.

Les efforts internationaux en matière de cybersécurité permettent de mieux comprendre la nature des menaces et les moyens pour y répondre. Les exercices Cyber Europe ou Locked Shields de l'Organisation du Traité de l'Atlantique Nord sont un cas d'espèce.

Il ne faut pas sous-estimer la valeur de la participation au dialogue international des parties prenantes représentant les organisations non gouvernementales, les entreprises et la communauté universitaire.

Portugal

[Original : anglais]
[31 mai 2016]

Dans sa résolution 70/237 intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », l'Assemblée générale a rappelé le rôle de la science et de la technologie dans le contexte de la sécurité internationale, et a notamment constaté que les innovations dans ces domaines pouvaient se prêter à des applications tant civiles que militaires. 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. À cet égard, 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-nations.

Dans la même résolution, l'Assemblée générale a invité les États Membres à collaborer dans quatre domaines, en rappelant le rapport de 2015 du Groupe d'experts gouvernementaux, à savoir :

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

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

c) Les principes destinés à renforcer la sécurité des systèmes mondiaux de télécommunications ;

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

Le rapport figurant dans le document A/68/98 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, le Portugal sait part de ses observations, comme suit :

I. Normes, règles et principes de comportement responsable des États

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

2. Nous devons 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 imposent de signaler les violations de la sécurité ou les atteintes à l'intégrité dont les répercussions sur le fonctionnement des services sont loin d'être négligeables.

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

4. Au plan international, il importe de renforcer les échanges d'informations et d'effectuer des exercices de formation sur le terrain dans les zones frontalières.

II. Mesures de renforcement de la confiance et échange d'informations

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

2. 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 technique et l'organisation de conférences et de séminaires auxquels sont parfois invités des conférenciers internationaux.

III. Mesures de renforcement des capacités

1. 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.

2. 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.

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

[Original : anglais]
[31 mai 2016]

Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord se félicite de l'occasion qui lui est donnée de donner son avis au sujet de la résolution 70/237 de l'Assemblée générale intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », dans le sillage de sa contribution concernant la résolution 69/28 de 2015. 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 que le cyberespace constitue un élément clef d'infrastructures nationales et internationales vitales et qu'il est le socle essentiel des activités économiques et sociales en ligne. Le Royaume-Uni fait allusion à l'évaluation des risques de sécurité au niveau national de 2015 qui a confirmé que le

cyberespace continuait de représenter une menace du premier degré à la sécurité nationale. Au financement de 860 millions de livres Sterling consacré par le Royaume-Uni à la stratégie nationale de cybersécurité précédente (2011-2016) s'ajoutera une enveloppe supplémentaire de 1,9 milliard de livres Sterling au cours des cinq prochaines années. Une nouvelle stratégie nationale de cybersécurité sera publiée en 2016, prévoyant la mise en place d'un nouveau Centre national de cybersécurité.

Le Royaume-Uni est conscient que la collaboration internationale est essentielle à l'efficacité de la cybersécurité. Nous continuons à promouvoir un cyberespace libre, ouvert, pacifique et sûr de sorte que ses avantages économiques et sociaux soient protégés et bénéficient à tous. Le Royaume-Uni montre l'exemple en relevant les défis de la cybersécurité transfrontalière par des initiatives telles que l'Alliance mondiale WePROTECT pour mettre fin à l'exploitation sexuelle en ligne des enfants. Par ailleurs, nous nous sommes engagés à mutualiser les meilleures pratiques internationales et veiller à ce que la communauté mondiale ait accès à l'assistance pour développer ses capacités en matière de cybersécurité.

Le Royaume-Uni continue de participer activement et de manière constructive au 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 qu'en réaffirmant que le droit international s'applique au cyberespace et que le respect par les États du droit international, en particulier leurs obligations découlant de la Charte des Nations Unies, est un cadre essentiel pour leurs actions dans l'utilisation des technologies de l'information et de la communication, le rapport consensuel du dernier groupe constitue un progrès significatif.

En outre, le Royaume-Uni se félicite de la poursuite des discussions concernant d'éventuelles futures mesures de confiance dans le cyberespace au sein de l'Organisation pour la sécurité et la coopération en Europe et les travaux similaires dans d'autres organisations régionales.

Le Royaume-Uni se réjouit 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.

Serbie

[Original : anglais]
[31 mai 2016]

La République de Serbie attache la plus grande importance à l'instauration et au développement de la cybersécurité et considère qu'il s'agit là d'une des priorités stratégiques de la société de l'information.

L'Assemblée nationale de la République de Serbie a adopté une loi sur la cybersécurité en janvier 2016. Cette loi prévoit la création de l'autorité compétente en matière de cybersécurité, qui aura pour missions d'élaborer la réglementation en conformité avec les normes nationales et internationales, de coopérer avec les autorités compétentes des autres pays et de surveiller son application. La loi sur la

cybersécurité définit les systèmes des technologies de l'information et des communications (TIC) qui ont une importance particulière en Serbie, et pour lesquels les opérateurs devront prendre des mesures techniques et organisationnelles adéquates pour assurer la cybersécurité informatique. Il s'agit des systèmes suivants : a) les systèmes de TIC des organismes publics; b) les systèmes de traitement des données personnelles sensibles; c) les systèmes de TIC dans les domaines d'intérêt public (énergie, transport, gaz, services bancaires, systèmes de santé et autres).

L'autorité compétente participe à la coopération internationale et, en particulier, alerte sur les risques et les incidents qui : a) sont en croissance rapide ou ont tendance à devenir des risques élevés; b) dépassent les capacités nationales; c) peuvent avoir des conséquences pour plus d'un pays.

La loi prévoit la mise en place d'une équipe d'intervention en cas d'urgence informatique au sein de l'Autorité de régulation des communications électroniques et des services postaux, qui, entre autres fonctions, coopère avec les organismes similaires d'autres pays.

La loi encadre également la cryptosécurité et la protection contre les émanations électromagnétiques nocives.

Afin de renforcer la sécurité des systèmes mondiaux d'information et de télécommunications, les États doivent coopérer, notamment en mettant en place des mécanismes d'intervention efficaces et adaptés pour l'échange d'informations, les alertes et les annonces sur les incidents de cybersécurité. À cette fin, les États devraient désigner des points focaux et en communiquer les coordonnées. Il convient d'accorder une attention particulière à la protection des infrastructures sensibles, en particulier si les incidents affectent le territoire de plusieurs États. Les États doivent également échanger les connaissances et coopérer en matière d'éducation dans ce domaine.

Compte tenu des risques accrus et des caractéristiques des cyberattaques dans l’espace virtuel, la communauté internationale devrait encourager les États à coopérer et à dialoguer pour renforcer leurs capacités en matière de cybersécurité et appuyer les organisations internationales qui assurent la coopération dans le domaine de la cybersécurité. La coopération efficace contribuera à rendre l'environnement mondial des TIC plus sûr et mieux protégé, un environnement où les États et les individus sont à l'abri des divers cyberrisques.

Suisse

[Original : anglais]
[7 juin 2016]

1. Ensemble des questions qui se posent en matière de sécurité informatique

Les technologies de l'information et de la communication (TIC) sont devenues un moteur indispensable des activités sociales, économiques et politiques. La Suisse s'est engagée à mettre à profit les possibilités qu’offrent les TIC. Cependant, l'utilisation de ces dernières expose l'infrastructure de l'information et des communications aux activités criminelles ou terroristes qui touchent le renseignement et la sphère politico-militaire et compromettent le fonctionnement

des équipements. Les perturbations, la manipulation et les attaques spécifiques perpétrées à travers les réseaux électroniques sont des risques auxquels la société de l'information est exposée.

2. Efforts déployés au niveau national pour renforcer la sécurité informatique et promouvoir la coopération internationale dans ce domaine

En 2012, le gouvernement fédéral suisse a adopté la Stratégie nationale pour la protection de la Suisse contre les cyberrisques, jetant ainsi les bases d'une approche globale de cette question. Cette stratégie vise à améliorer la détection précoce des cyberrisques et les menaces émergentes, à rendre l'ensemble de l'infrastructure suisse plus résistante aux cyberattaques et, de manière générale, à réduire les cyberrisques. Elle reflète, d'autre part, la nécessité d'une culture de la cybersécurité, de la responsabilité partagée de tous les participants et d'une approche fondée sur le risque. En outre, elle préconise la coordination au niveau gouvernemental et la coopération nationale (partenariat public-privé) et internationale. La stratégie comprend 16 mesures. Le gouvernement fédéral suisse a adopté en 2013 un plan détaillé pour la mise en œuvre de la Stratégie nationale pour la protection de la Suisse contre les cyberrisques.

3. Principes visés au paragraphe 3 (de la résolution)

Les cyberrisques doivent être contrés grâce à la coopération internationale renforcée (sphère d'action 5 définie par la stratégie). La politique extérieure de la Suisse en matière de cybersécurité porte sur l'élaboration de normes de comportement responsable des États, les mesures de confiance et le renforcement des capacités. Dans cette optique, la Suisse participe à différents processus internationaux. L'Organisation pour la sécurité et la coopération en Europe (OSCE) a adopté des mesures de confiance dans le domaine de la cybersécurité. La Suisse considère que ce processus revêt une importance capitale. D'autre part, la Suisse participe au processus de Londres, qui est tout aussi important. La Suisse soutient une série de projets de renforcement des capacités.

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

Toutes les mesures prises par la communauté internationale visent un équilibre entre les impératifs de sécurité et les aspects liés aux droits humains. Les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne. Les mesures destinées à créer la confiance et à la renforcer restent encore à élaborer. L'ensemble des mesures de confiance adoptées par l'OSCE sont d'une importance capitale pour le renforcement de la sécurité. L'instauration de la transparence par l'échange d'informations, le renforcement de la coopération et les activités pratiques et conjointes contribuera à la stabilité globale du cyberespace.

Togo

[Original : français]
[2 juin 2016]

Bien que le progrès de l'information et des télécommunications constitue un atout considérable pour le développement des pays, il reste, dans le même temps, une menace pour la sécurité nationale et internationale. C'est un espace virtuel qui est souvent utilisé à des fins criminelles ou terroristes.

Le Togo n'est pas à l'abri de cette menace et connait déjà une criminalité liée aux technologies de l'information et de la communication, criminalité qui va des cas d'escroquerie et autres fraudes à la pédopornographie et atteintes à la liberté et à l'intégrité des personnes.

À l'heure du terrorisme, le web et les réseaux sociaux demeurent un lieu de propagande et de recrutement pour des organisations terroristes. À cela s'ajoute le fait que la plupart des pays migrent vers une administration électronique, ce qui constitue un défi majeur pour nos gouvernements, qui redoutent des cyberattaques qui porteraient atteinte au bon fonctionnement des administrations et à la sécurité dans les domaines civils et militaires.

Face à cette situation, il importe que des mesures soient prises au niveau international et national pour maîtriser le secteur de l'informatique et des télécommunications à travers un contrôle permettant de lutter contre son usage à des fins criminelles.

Au Togo, plusieurs mesures ont été prises dans ce sens, notamment :

- L'adoption du décret N°2011-120/PR du 6 juillet 2011 portant identification systématique et obligatoire des abonnés aux services de télécommunications ;
- L'adoption de la loi N°2012-018 sur les communications électroniques et la loi N°2013-003 la modifiant ;
- L'élaboration des avant-projets de loi sur la cybercriminalité, la cryptographie, la cybersécurité, la protection des données à caractère personnel et sur les transactions électroniques.

L'objectif de cette réglementation est d'assurer la traçabilité de toute activité informatique et de télécommunication et de mettre en place un dispositif de sécurité qui permet de protéger les réseaux informatiques et de télécommunication contre toute intrusion frauduleuse.

Le Togo a jugé également nécessaire de mettre en place un cadre institutionnel qui assure le contrôle. Ainsi, un centre national de traitement des incidents informatiques afin de disposer, au plan national, d'une veille en matière de cybersécurité. Ce centre viendra compléter l'action de l'Autorité de réglementation des secteurs des postes et télécommunications.

En plus, il convient de mentionner le renforcement de capacités humaines entrepris pour permettre aux services de répressions et entités publiques et privées impliqués dans la cybersécurité d'agir efficacement contre toute sorte de menace.

Par ailleurs, la coopération internationale notamment dans le cadre de l'Union internationale des télécommunications et l'Organisation des Nations Unies permettra de parvenir à plus de sécurité dans l'informatique et les télécommunications.

Turkmenistan

[Original : russe]
[28 mars 2016]

La politique intérieure et extérieure du Turkménistan repose sur le principe de neutralité, basée sur les liens étroits entre les intérêts nationaux, la sécurité

mondiale et le progrès universel. La nature pacifique de sa politique intérieure est un précepte fondamental pour le Turkménistan, découlant de son principe de neutralité et de ses obligations internationales. Ainsi, le Turkménistan traite toutes ses affaires uniquement par les voies politique et diplomatique, essentiellement par le truchement de l'Organisation des Nations Unies et d'autres organisations internationales. Le Turkménistan appuie pleinement les efforts internationaux en matière de lutte contre la prolifération des armes de destruction massive, de leurs vecteurs et des technologies connexes et considère le désarmement comme une condition fondamentale à la sécurité mondiale. Le Turkménistan stipule dans sa législation son refus de posséder, de produire, de stocker ou de transporter tout type d'armes de destruction massive, qu'elle soit nucléaire, chimique, bactériologique ou autre, y compris les nouveaux types d'armes et les techniques de leur fabrication.

Le Turkménistan adhère à plusieurs instruments juridiques internationaux relatifs au désarmement et visant à préserver la paix universelle, l'harmonie et la sécurité dans le monde entier, par l'engagement des États Membres.

Conformément à l'importance qu'il accorde au renforcement de la paix et de la sécurité internationales, le Turkménistan appelle à réduire les stocks d'armes. Le peuple turkmène est convaincu que moins il y aura d'armes dans le monde, plus son développement sera stable et pacifique et plus les pays et les peuples se feront confiance et se comprendront.

Comme annoncé dans son concept de politique étrangère 2013-2017, le Turkménistan continuera à faciliter activement le processus de désarmement et de réductions des arsenaux, notamment des armes de destruction massive.

Lors de son discours à la réunion du Conseil des ministres du 5 juin 2015, le Président du Turkménistan a attiré particulièrement l'attention sur les obligations de notre pays envers la communauté mondiale. Il a rappelé que le principe de neutralité signifiait la non-adhésion aux alliances et blocs politiques, économiques et militaires, une armée dont les capacités se limitent à assurer la protection de la paix et de la liberté de la nation, le rejet des armes de destruction massive, et l'interdiction de transporter telles armes dans notre pays, par voie terrestre ou aérienne, l'adhésion aux valeurs universelles et aux principes démocratiques, la garantie de la paix civile et de l'harmonie dans le pays et la coopération avec l'Organisation des Nations Unies et les organisations humanitaires internationales.

La reconnaissance unanime de la résolution 69/285 sur la neutralité permanente du Turkménistan par 193 États Membres, lors de la soixante-neuvième session de l'Assemblée générale des Nations Unies du 3 juin 2015, illustre la reconnaissance universelle des politiques efficaces visant à garantir la paix, la sécurité et le développement durable aux niveaux régional et international. Cette résolution souligne la pertinence de la neutralité permanente du Turkménistan pour le renforcement de la paix et de la sécurité régionales, ainsi que la contribution de notre pays au développement de relations amicales et bénéfiques à l'ensemble des pays du monde.

Pays hôte du siège du Centre régional des Nations Unies pour la diplomatie préventive en Asie centrale, le Turkménistan appelle à un engagement plus actif de ce Centre dans plusieurs domaines relatifs aux problèmes de la région, avec l'appui des États Membres de l'ONU et d'organisations internationales (notamment

l'Organisation pour la sécurité et la coopération en Europe, l'Union européenne et Communauté d'États indépendants).

Un forum international sur la sauvegarde de la paix, de la stabilité et de la sécurité en Asie centrale s'est tenu avec succès à Achgabat en 2015. En tant que partie aux traités, conventions et instruments multilatéraux des Nations Unies relatifs au désarmement, le Turkménistan entend continuer à apporter toute son assistance dans ce domaine, notamment à l'échelon régional, et à accueillir régulièrement des réunions régionales sur le thème du désarmement en Asie centrale.