Nations Unies A/69/112/Add.1

Assemblée générale

Distr. générale
18 septembre 2014
Français
Original : anglais/espagnol/français

Soixante-neuvième session
Point 92 de l'ordre du jour provisoire*
Progrès de l'informatique et des télécommunications et sécurité internationale

Progrès de l'informatique et des télécommunications et sécurité internationale

Rapport du Secrétaire général

Additif**

Table des matières

Page

II. Réponses reçues des gouvernements 2
Canada 2
Espagne 3
France 4
République de Corée 5
Suède 6

* A/69/150.

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

14-61130 (F) 270914 290914

Merci de recycler

II. Réponses reçues des gouvernements

Canada

[Original : anglais]
[12 juin 2014]

Le Canada souhaite faire part des vues suivantes au Secrétaire général, compte tenu du rapport de 2013 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (A/68/98). Moteur de la croissance économique, de l'innovation et du développement social, le cyberespace a renforcé les interactions sociales et transformé le secteur privé et les gouvernements. Il a également engendré de nouvelles menaces et des problèmes de société, comme le harcèlement en ligne, la cybercriminalité et l'utilisation d'Internet à des fins terroristes.

Le Canada salue le fait que, dans le rapport de 2013 du Groupe d'experts gouvernementaux, 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.

Le Canada est fermement déterminé à favoriser un Internet libre et ouvert à tous, pour sa prospérité économique, mais aussi pour soutenir ses valeurs et ses intérêts et protéger la sécurité de ses citoyens.

Parmi les efforts déployés par le Canada au niveau national, l'application de sa Stratégie de cybersécurité et de son Plan d'action en la matière contribue à sécuriser ses systèmes cybernétiques et à protéger les Canadiens en ligne grâce à la collaboration active des secteurs des infrastructures essentielles, comme les finances, les transports et l'énergie.

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.

Il coopère étroitement avec ses partenaires multilatéraux et avec le secteur privé pour renforcer la sécurité de l'information sur les réseaux dont dépendent la bonne santé économique et la sécurité du pays.

Sur le plan international, le Canada s'est engagé à verser plus de 3,6 millions de dollars à l'Organisation des États américains pour la période 2007-2016 en vue de renforcer les capacités en matière de cybersécurité des pays membres de l'Organisation, y compris en mettant en place des équipes d'intervention en cas d'urgence liée à la sécurité informatique.

Dans le cadre de l'Organisation pour la sécurité et la coopération en Europe, le Canada a participé à l'élaboration d'un ensemble de mesures de confiance et de sécurité afin de réduire les risques de conflit lié à l'utilisation de l'informatique et des télécommunications dans le cyberespace.

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.

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'information aux niveaux stratégique et opérationnel.

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. Il est membre de l'Alliance mondiale contre les abus sexuels commis contre des enfants via Internet et a participé aux travaux menés par le Groupe d'experts gouvernementaux en 2012-2013.

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.

Il est convaincu que le renforcement de la sécurité informatique doit aller de pair avec le respect des droits de l'homme et des libertés fondamentales. Les droits dont les citoyens jouissent hors ligne, comme la liberté d'expression, d'association et de réunion et le respect de la vie privée, doivent aussi être protégés en ligne.

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

Espagne

[Original : espagnol]
[30 juin 2014]

L'Espagne estime que les gouvernements doivent promouvoir et préserver un cyberespace ouvert, accessible et sûr, tout en protégeant les valeurs fondamentales telles que la démocratie, les droits de l'homme et l'état de droit.

La cybersécurité est une priorité stratégique pour l'Espagne. Aussi, dans la droite ligne des stratégies en la matière adoptées par ses partenaires de l'Union européenne, l'Espagne a adopté le 5 décembre 2013 une Stratégie nationale de cybersécurité qui définit une démarche intégrée et établit un système de coordination interministériel, le Conseil national de la cybersécurité, chargé d'intervenir en cas de crise.

La Stratégie prévoit également des mesures de coopération internationale ainsi que la participation d'organisations et d'entreprises, en particulier de celles ayant un caractère stratégique. Les activités d'éducation et de sensibilisation visant à accroître la connaissance qu'a la société civile des questions de cybersécurité figurent parmi ses principales composantes.

L'Espagne considère que l'Organisation des Nations Unies a un rôle primordial à jouer pour ce qui est de parvenir à un consensus international dans ce domaine et appuie la tenue d'un débat institutionnalisé dans le cadre de l'Organisation afin de garantir une utilisation pacifique et sûre de l'informatique. Elle appuie également les recommandations formulées par le Groupe d'experts gouvernementaux de l'Organisation dans son rapport de 2013.

C'est dans cet objectif que l'Espagne a organisé une réunion sur la cybersécurité, au niveau des représentants permanents, le 21 mars 2014 à Madrid.

Elle participe aussi au Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale et prend activement part à diverses initiatives internationales dans le domaine de la sécurité dans le cadre, entre autres, de l'Organisation pour la sécurité et la coopération en Europe, de l'Organisation du Traité de l'Atlantique Nord, de l'Office des Nations Unies contre la drogue et le crime, du Conseil des droits de l'homme de l'Organisation des Nation Unies et des Conférences « Meridian » sur la protection des infostructures essentielles. En outre, l'Espagne est partie à la Convention de Budapest sur la cybercriminalité.

L'Espagne estime que pour renforcer la sécurité de l'information à l'échelle mondiale, la communauté internationale devrait adopter des mesures dans quatre domaines d'activité :

1) Renforcement de la confiance : il faut accroître la transparence, améliorer l'échange d'information et adopter des pratiques optimales;

2) Droit international : la communauté internationale et, en particulier, l'Organisation des Nations Unies, devraient continuer d'examiner la façon dont les principes et normes du droit international peuvent être interprétés et appliqués dans le contexte du cyberespace;

3) Coopération internationale : il faut améliorer les mécanismes de communication en cas d'incident et renforcer les dispositifs de coopération policière et judiciaire, qui doivent être plus souples;

4) Renforcement des capacités : il faut renforcer les capacités des pays qui en ont besoin dans le cadre d'activités bilatérales et d'organisations internationales.

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

France

[Original : français]
[15 septembre 2014]

À titre préliminaire, la France souhaite rappeler qu'elle n'emploie pas le terme de « sécurité de l'information », auquel elle préfère le terme de « sécurité des systèmes d'information » ou encore de « cybersécurité ». Active dans la promotion du principe de liberté d'expression en ligne (Résolution 20/8 du Conseil des droits de l'Homme de 2012), la France n'estime pas que l'information en tant que telle puisse être un facteur de vulnérabilité contre laquelle il est nécessaire se protéger, hormis dans les conditions strictement établies par la loi, de manière proportionnée et transparente, conformément à l'article 19 du Pacte relatif aux droits civils et politiques.

Le fonctionnement de notre société dépend de manière croissante des systèmes d'information et des réseaux, notamment d'Internet. Une attaque réussie contre un système d'information critique pourrait donc entraîner des conséquences humaines ou économiques graves. C'est pourquoi la France a défini en 2011 une Stratégie pour la défense et la sécurité des systèmes d'information, érigeant ainsi la cybersécurité en véritable priorité nationale. Le Livre blanc sur la Défense et la Sécurité nationale de 2013 est venu affiner notre perception de la menace en

identifiant deux dangers majeurs pour la nation : le cyberespionnage et le cybersabotage d'infrastructures d'importance vitale.

Créée en 2009 pour répondre à ces défis, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a depuis connu un constant renforcement de ses moyens et de ses prérogatives. Elle porte aujourd'hui, au nom du Premier Ministre, l'ensemble des missions de prévention et de réaction relatives à la cybersécurité de nos infrastructures critiques, y compris gouvernementales. Responsable de la sécurité de ses propres réseaux, le Ministère de la défense est également monté en puissance dans ce domaine, comme l'illustre la parution d'un ambitieux document stratégique en février 2014, le « Pacte Défense Cyber ».

En parallèle, la France s'est engagée activement à renforcer la coopération internationale en matière de cybersécurité, sans laquelle les efforts nationaux sont limités. Depuis le G8 de Deauville en 2011, elle est particulièrement attachée à renforcer la régulation internationale du cyberespace. Dans ce but, elle participe aujourd'hui activement aux travaux du Groupe d'experts gouvernementaux de l'Organisation des Nations Unies et de l'Organisation pour la sécurité et la coopération en Europe visant à mettre en place un cadre normatif international reposant sur le droit international existant, ainsi que des mesures de confiance et des normes de comportement spécifiques au cyberespace. Enfin, la France s'applique à mettre en œuvre l'objectif de renforcement international des capacités en matière de cybersécurité, au travers de programmes concrets initiés dans un cadre bilatéral ou multilatéral (Union européenne, Organisation du Traité de l'Atlantique Nord).

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

République de Corée

[Original : anglais]
[30 juin 2014]

Le cyberespace offre un nombre infini de possibilités permettant d'accroître le développement économique et social et la prospérité partout dans le monde. Il doit être ouvert et sûr pour faire progresser l'humanité et promouvoir la participation démocratique, mais il est aussi à l'origine de nouvelles menaces, comme la cybercriminalité, le cyberterrorisme et la cyberguerre.

Afin de résoudre ces problèmes, le Gouvernement de la République de Corée a annoncé l'adoption, en juillet 2013, d'un ensemble complet de contre-mesures qui visent à renforcer la cybersécurité nationale en déterminant la réponse à adopter en cas de cyberattaque et en recensant les moyens de renforcer la sécurité de certaines infostructures vitales.

La République de Corée est d'avis que la coopération internationale devrait se concentrer sur l'élaboration, à l'échelle internationale, d'une série de normes et de mesures de confiance, sur le renforcement des capacités cybernétiques des pays en développement et sur la promotion de la coopération entre les équipes d'intervention informatique d'urgence.

Le Gouvernement coréen tient régulièrement des consultations bilatérales à ce sujet avec plusieurs pays et participe activement aux débats régionaux et

internationaux sur ces questions, y compris dans le cadre du Forum régional de l'Association des nations de l'Asie du Sud-Est, du Sommet sur la sécurité nucléaire et de l'Organisation des Nations Unies. Plus récemment, les 17 et 18 octobre 2013, la République de Corée a accueilli la Conférence de Séoul sur le cyberespace, qui faisait suite à celles organisées à Londres en 2011 et à Budapest en 2012. Cette conférence a permis de sensibiliser les participants à la nécessité de renforcer la coopération internationale afin de faire face aux menaces croissantes et de trouver un terrain d'entente pour résoudre les principaux problèmes de cybersécurité. Les pays participants ont adopté le Cadre et les engagements de Séoul pour un cyberespace ouvert et sûr, inclus dans le résumé du Président.

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

Suède

[Original : anglais]
[12 septembre 2014]

L'essor du cyberespace engendre un nombre illimité de possibilités, mais l'utilisation de l'informatique et des télécommunications comporte aussi des problèmes de sécurité qu'il faut résoudre grâce à la coopération internationale.

En Suède, les travaux sur la stratégie nationale de sécurité informatique ont évolué au fil du temps et le Gouvernement travaille actuellement à une stratégie nationale en matière de cybersécurité. La Commission de la défense suédoise a récemment réalisé des évaluations relatives à la cybersécurité et à la cyberdéfense et souligné que la Suède devait renforcer ses capacités globales en la matière.

La Suède participe activement à plusieurs instances internationales œuvrant dans le domaine du cyberespace et cherche à mettre en place des dialogues bilatéraux et régionaux sur les questions cybernétiques, y compris avec les pays nordiques et baltiques. Elle s'est en particulier attachée à promouvoir les droits de l'homme dans le contexte du cyberespace et à favoriser un modèle multipartite de gouvernance de l'Internet, et estime que les activités de surveillance internationale doivent reposer sur des principes fondamentaux.

La Suède est partisane d'une politique européenne homogène en matière de cybercriminalité, fondée sur les valeurs et les intérêts fondamentaux de l'Union européenne (UE). L'adoption, en 2013, de la Stratégie globale de l'UE en matière de cybersécurité a constitué un progrès important. La Suède est l'un des pays fondateurs de la Coalition pour la liberté en ligne, qui a pour objectif de faire progresser la liberté sur Internet dans le monde entier. Pendant trois années consécutives, elle a accueilli le Stockholm Internet Forum, une conférence multipartite visant à approfondir l'examen des questions liées à la liberté sur Internet et au développement mondial de cet outil. La Suède fait partie du petit groupe d'États à l'origine de la résolution 20/8 (2012) du Conseil des droits de l'homme, dans laquelle celui-ci a affirmé que les droits dont les personnes jouissaient hors ligne devaient également être protégés en ligne. Pendant trois années consécutives, la Suède a présenté des déclarations communes à la Première Commission de l'Assemblée générale, soulignant notamment que le renforcement de la sécurité informatique et internationale devait reposer sur une démarche

multipartite soucieuse des droits de l'homme. Elle a aussi activement contribué à l'adoption du premier ensemble de mesures de confiance de l'Organisation pour la sécurité et la coopération en Europe visant à réduire les risques de conflit lié à l'utilisation de l'informatique et à accroître la transparence en accordant une attention particulière au respect et à la promotion des droits de l'homme.

Il faut faire des efforts à l'échelle mondiale en vue de définir les principes de base qui régiront l'utilisation de l'informatique et les relations internationales dans le cyberespace. On trouvera ci-dessous certaines propositions à ce sujet. Afin de renforcer la cybersécurité, la communauté internationale et l'ensemble des parties prenantes doivent collaborer sur des projets concrets, comme la création d'un ensemble de règles volontaires ou de normes de bonne conduite internationale dans le cyberespace. Les acteurs mondiaux devraient travailler à l'élaboration de mesures de confiance afin d'accroître la transparence et la prévisibilité et de réduire par là même le risque de malentendu ou de conflit dans le cyberespace.

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