Nations Unies A/69/112

Assemblée générale

Distr. générale
30 juin 2014
Français
Original : anglais/espagnol

Soixante-neuvième session
Point 92 de la liste préliminaire*
Progrès de l'informatique et des télécommunications et sécurité internationale

Progrès de l'informatique et des télécommunications et sécurité internationale

Rapport du Secrétaire général

Table des matières

* A/69/50.

14-56479 (F) 250714 250714

I. Introduction

1. Le 27 décembre 2013, l'Assemblée générale a adopté la résolution 68/243 intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale ». Au paragraphe 3 de sa résolution, l'Assemblée générale a invité tous les États Membres à continuer de communiquer au Secrétaire général, en tenant compte des constatations et recommandations figurant dans le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de 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 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'échelon mondial.

2. Pour donner suite à cette demande, une note verbale a été adressée aux États Membres le 19 février 2014 pour les inviter à communiquer des informations à ce sujet. Les réponses reçues 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]
[30 mai 2014]

Résumé analytique

Les outils télématiques offrent des possibilités sans précédent aux pays industrialisés comme aux pays en développement, mais ils se caractérisent par une certaine vulnérabilité et des faiblesses systémiques.

Il existe une tendance à des activités malveillantes, sophistiquées et difficiles à détecter visant des objectifs de grande valeur. Il peut en résulter de graves conséquences. Une attaque électronique contre des infrastructures essentielles peut être plus perturbatrice qu'une attaque physique ponctuelle et avoir des conséquences imprévisibles pour les autres entités raccordées au même réseau.

Malgré ces risques, l'éventualité d'une cyberguerre totale semble peu probable à l'heure actuelle. Il est plus vraisemblable que des moyens cybernétiques limités soient utilisés dans le cadre d'une guerre plus vaste. Enfin, il existe le danger que des attaques informatiques ne dégénèrent en conflit véritable.

Face à ces risques, il devient de plus en plus important de renforcer la résilience informatique, de convenir de lois et règlements applicables à l'usage des moyens télématiques et d'établir des mesures de confiance.

Des progrès ont été accomplis en 2013 : dans son dernier rapport, le Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale a clairement établi que le droit international s'applique au cyberespace. Il a également conclu que la souveraineté de l'État et les normes et principes internationaux qui en découlent s'appliquent à l'utilisation de l'outil informatique par les États ainsi qu'à leur compétence territoriale en matière d'infrastructure informatique. L'Allemagne attend avec intérêt la poursuite des travaux du Groupe d'experts gouvernementaux.

En ce qui concerne les mesures de confiance, l'Organisation des Nations Unies, l'Organisation pour la sécurité et la coopération en Europe (OSCE) a fait de gros progrès en adoptant un premier train de mesures visant à renforcer la coopération entre les États, la transparence, la prévisibilité et la stabilité afin de réduire les risques d'erreur d'interprétation, d'envenimement des situations et des conflits pouvant découler de l'emploi des technologies de l'information et des télécommunications. L'accord de l'OSCE pourrait servir de modèle à d'autres organisations régionales.

La Stratégie allemande en matière de cybersécurité (2011) est fondée sur le postulat que l'ouverture du cyberespace et l'intégrité, l'authenticité et la confidentialité des données dans cet espace revêtent aujourd'hui une importance capitale. La cybersécurité est primordiale pour l'État, les entreprises et la société. Tous doivent agir de concert, à la fois à l'échelon national et en coopération avec leurs partenaires internationaux. La stratégie allemande de cybersécurité définit les objectifs et mesures suivants :

- Protéger les infrastructures informatiques essentielles;
- Sécuriser les systèmes informatiques;
- Renforcer la sécurité informatique dans l'administration publique;
- Créer un centre national d'intervention informatique;
- Établir un conseil national de la cybersécurité;
- Lutter efficacement contre la cybercriminalité;
- Promouvoir une action coordonnée efficace pour assurer la cybersécurité en Europe et dans le monde;
- Employer des technologies informatiques fiables et sûres;
- Assurer la formation professionnelle du personnel des autorités fédérales;
- Mettre en place des dispositifs d'intervention en cas d'attaque informatique.

Après les élections générales allemandes de septembre 2013 et conformément à l'accord de coalition conclu ensuite, la cybersécurité est devenue l'une des priorités du Gouvernement. Les normes en matière de confidentialité des données seront renforcées. Les principales priorités pour les quatre prochaines années sont les suivantes : mieux protéger les consommateurs, modifier la législation pénale pour mieux protéger les personnes, adopter une loi sur la sécurité informatique fixant des normes de sécurité minimales obligatoires pour les infrastructures essentielles, et faire obligation à toutes les autorités fédérales de consacrer 10 % de leur budget informatique à l'amélioration de la sécurité de leurs systèmes.

Face aux craintes de surveillance illégale ou arbitraire ou d'interception des communications ainsi que de collecte illégale ou arbitraire de données personnelles par des tiers, le Gouvernement allemand encourage vivement les prestataires de services informatiques à crypter les télécommunications et à s'abstenir de communiquer des données à leur sujet aux services de renseignement étrangers.

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

Australie

[Original : anglais]
[30 mai 2014]

Pour l'Australie, le droit international tel qu'il existe offre le cadre nécessaire pour régir le comportement des États dans le cyberespace et déterminer les mesures appropriées à prendre en cas d'activités en ligne illégales menées par des États. Le droit international englobe, selon le cas, le droit international humanitaire, le droit régissant l'usage de la force, le droit international des droits de l'homme et le droit international relatif à la responsabilité des États. Toute norme nouvelle concernant le comportement des États dans le cyberespace doit être élaborée en conformité avec le droit international.

Le rapport consensuel du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (A/68/98) a grandement contribué à guider les États en affirmant que le droit international, et en particulier la Charte des Nations Unies, s'applique à l'utilisation par les États du cyberespace et est essentiel pour le maintien de la paix et de la stabilité. L'Australie considère que cette conclusion revêt une importance fondamentale. Elle estime que les États doivent, individuellement et collectivement, réaffirmer publiquement que le droit international s'applique au comportement des États dans le cyberespace et qu'ils s'engagent à agir dans le cyberespace conformément à leur interprétation du droit international.

Le rapport reconnaît la nécessité de débattre plus avant et de préciser les modalités d'application du droit international à l'utilisation par les États du cyberespace et recommande de poursuivre l'étude de cette question. Il souligne que des normes supplémentaires pourront être élaborées. L'Australie estime, sans pour autant sous-estimer la complexité de la tâche, que l'élaboration de modalités d'application du droit international au comportement des États dans le cyberespace dans les situations de conflit et hors conflit constitue une priorité pour la communauté internationale.

Le rapport formule également des recommandations novatrices pour l'adoption de mesures de confiance relatives au cyberespace. L'Australie reconnaît que l'élaboration de modalités d'application du droit international à l'utilisation par les États du cyberespace est une tâche à long terme. Dans l'immédiat, il importe que des mesures pratiques soient prises pour régler et prévenir les problèmes entre États relatifs au cyberespace, qui peuvent résulter de malentendus et déboucher ensuite sur un conflit du fait d'erreurs d'interprétation et de l'escalade qui a suivi. Les organisations régionales de sécurité sont particulièrement bien placées pour étudier, élaborer et appliquer des mesures de confiance concernant le cyberespace. Au sein

du Forum régional de l'Association des nations de l'Asie du Sud-Est, l'Australie dirige des travaux sur ce sujet important; compte tenu du niveau inégal des capacités des membres, il conviendrait de fixer des objectifs pour leur renforcement.

Autriche

[Original : anglais]
[19 mai 2014]

La stratégie adoptée en mars 2013 par l'Autriche en matière de cybersécurité offre un cadre global et dynamique pour la protection du cyberespace ainsi que des personnes opérant dans cet espace virtuel tout en garantissant le respect des droits de l'homme. Elle améliore la sécurité et la résilience des infrastructures et services autrichiens dans le cyberespace. Aspect très important, elle permet de sensibiliser la société autrichienne et d'en accroître le degré de confiance.

La stratégie autrichienne attache une importance majeure à l'établissement de réseaux à l'échelle mondiale et à la coopération internationale. Elle vise à assurer la sécurité du cyberespace par un mélange de mesures coordonnées aux niveaux national et international. L'Autriche entend mener, selon une approche coordonnée et ciblée, une « politique étrangère cybernétique » active dans le cadre de partenariats avec l'Union européenne, l'Organisation des Nations Unies, l'OSCE et l'Organisation du Traité de l'Atlantique Nord (OTAN).

L'Autriche contribuera activement à la mise en œuvre de la stratégie de cybersécurité de l'Union européenne en participant pleinement à ses activités stratégiques et opérationnelles. Les ministères compétents prendront les mesures nécessaires pour appliquer et utiliser à plein la Convention du Conseil de l'Europe sur la cybercriminalité. L'Autriche défend la gratuité de l'Internet au niveau international. Le libre exercice de tous les droits humains doit être garanti dans cet espace virtuel; en particulier le droit à la liberté d'expression et d'information ne doit pas être indûment restreint sur Internet.

L'Autriche poursuivra sa coopération bilatérale dans le cadre de son partenariat avec l'OTAN et appuiera activement l'élaboration d'une liste de mesures concrètes de confiance et de sécurité à l'OSCE. Elle participe activement à la planification et à l'exécution d'exercices cybernétiques transnationaux. L'expérience acquise servira directement à la planification et à la promotion d'une coopération opérationnelle. Le Ministère des affaires étrangères coordonne les mesures de politique étrangère relatives à la cybersécurité. Le cas échéant, la signature d'accords bilatéraux ou internationaux sera envisagée.

Sur le plan national, un groupe directeur élabore actuellement un plan de mise en œuvre des mesures horizontales énoncées dans la stratégie autrichienne relative à la cybersécurité. En coordination avec le groupe directeur, les organismes compétents sont chargés de mettre en œuvre ces mesures et d'élaborer des sous-stratégies dans leur domaine respectif de responsabilité. Deux fois par an, les ministères représentés au sein du groupe directeur doivent présenter un plan de mise en œuvre au gouvernement fédéral. L'élaboration du plan s'accompagne d'un examen de la stratégie, laquelle est révisée et mise à jour selon les besoins.

Colombie

[Original : espagnol]
[23 mai 2014]

Ces dernières années, le développement et l'application des technologies de l'information et des communications ont fait de grands progrès, ce qui a engendré des changements et des bienfaits importants qui ont considérablement contribué au développement des pays et a favorisé l'expansion de la coopération internationale afin d'optimiser la diffusion de l'information.

Parallèlement, ces progrès suscitent une grande inquiétude quant à la possibilité de ce que cette évolution serve à ébranler la stabilité et la sécurité internationales et à nuire à l'intégrité de l'infrastructure des États, au détriment de la sécurité dans leurs secteurs civil et militaire.

Cela étant, pour la Colombie, le recours aux technologies nouvelles pour engendrer des menaces informatiques et la menace actuelle de la criminalité dans le cyberespace sont de graves préoccupations d'intérêt national.

Il lui est donc impératif de définir des politiques et stratégies afin d'éviter que les technologies de l'information soient utilisées à des fins terroristes ou criminelles.

Mesures prises au niveau national pour renforcer la sécurité de l'information et contribuer à la coopération internationale

Réponses normatives et institutionnelles

En 2005, la Colombie a élaboré la norme ISO-27001, conçue comme un système de gestion qui établissait des standards de qualité de la sécurité de l'information dans les entités nationales et favorisait la préservation des caractéristiques de confidentialité, d'intégrité et de disponibilité[1] de l'information.

En 2009, le Congrès de la République de Colombie a adopté la loi 1273 qui a modifié le Code pénal en créant un nouveau bien juridique protégé sous le titre « De la protection de l'information et des données ». Cette modification a permis de créer un cadre juridique national permettant aux entités compétentes de poursuivre en justice les crimes liés à l'utilisation des technologies de l'information.

Dans ce cadre, la Colombie punit notamment l'accès illicite, les interprétations illicites, les attaques contre l'intégrité des données, les attaques contre l'intégrité des systèmes, l'abus des dispositifs, la falsification informatique, la fraude informatique, la pédopornographie et les atteintes à la propriété intellectuelle et aux droits connexes.

En 2011, par le document CONPES 3701, la Colombie a mis en marche une politique et une stratégie nationales de cybersécurité et de cyberdéfense fondées sur trois piliers essentiels :

[1] Confidentialité : éviter que l'information ne soit utilisée par des personnes ou des voies non autorisées; intégrité : protéger la précision et la complétude de tout ce qui a de la valeur pour une organisation; disponibilité : information accessible et utilisable sur la demande des entités autorisées.

a) L'adoption d'un cadre institutionnel apte à faire face aux menaces et aux risques par la prévention, la coordination, le contrôle et l'élaboration de recommandations;

b) L'élaboration de programmes de formation et de spécialisation en matière de sécurité de l'information;

c) Le renforcement de la législation nationale dans ces domaines ainsi que celui de la coopération internationale. À cet égard, il faudra activer l'adhésion de la Colombie aux divers instruments internationaux comme la Convention sur la cybercriminalité (Convention de Budapest).

Afin de développer systématiquement les lignes stratégiques susvisées, la Colombie a créé et mis en marche quatre organismes :

1. La Commission intersectorielle, chargée d'esquisser la vision stratégique de la gestion de l'information ainsi que d'établir les grandes lignes de la gestion de l'infrastructure technologique de l'information publique, de la cybersécurité et de la cyberdéfense;

2. Le Groupe de riposte aux situations cybernétiques d'urgence en Colombie (colCERT), organe national de coordination pour la cybersécurité et la cyberdéfense;

3. Le Commandement cybernétique conjoint des forces armées (CCOC), chargé de prévenir et de contrecarrer toute menace ou attaque cybernétique visant les valeurs et les intérêts du pays;

4. Le Centre de police cybernétique, chargé de la cybersécurité du territoire colombien par le renseignement, l'aide et la protection contre les délits cybernétiques.

De plus, la Colombie dispose d'un cadre juridique pour la protection des données personnelles, créé en 2012 par la loi 1581 suivie en 2013 du décret 1377 qui en régit en partie l'application. Par ailleurs, il a été créé au Ministère de l'industrie et du commerce une Direction pour la protection des données personnelles.

D'autre part, le Ministère des technologies de l'information et des communications a mis au point et en œuvre la stratégie en ligne du Gouvernement qui regroupe les besoins des entités dans l'adoption de systèmes de gestion de la sécurité de l'information. En outre, depuis 2008, ce ministère a formé environ 6 300 fonctionnaires aux processus de gestion des technologies de l'information.

Enfin, il importe de préciser que, s'agissant des capacités, on progresse dans l'identification de l'infrastructure nationale primordiale (celle qui, si elle est touchée, risque de causer des pertes humaines et économiques ou de nuire à la gouvernabilité du pays) afin d'en préserver la sécurité cybernétique.

Coopération internationale

En 2013, la Colombie a officiellement demandé à adhérer à la Convention européenne sur la cybercriminalité qui fixe les principes de l'accord international sur la sécurité cybernétique et la sanction des crimes de cet ordre et dont l'objectif principal est de protéger la société contre la cybercriminalité par une législation idoine et par la coopération internationale.

De plus, en 2012, la Colombie a adhéré à un accord multilatéral avec le Forum mondial de l'économie intitulé « Alliance pour la résilience cybernétique » et destiné à recenser et à attaquer les risques mondiaux systématiques issus de la connectivité toujours plus grande entre les personnes, les processus et les objets.

Par ailleurs, le secrétariat du Comité interaméricain contre le terrorisme (CICTE) de l'Organisation des États américains s'est appliqué à renforcer les capacités des États membres en matière de cybersécurité. Son principal but a été de créer des groupes nationaux d'alerte, de vigilance et de prévention dits « équipes de riposte aux incidents » qui ont la mission et les moyens de faire face aux crises, aux incidents et aux menaces sur la sécurité cybernétique.

Dans ce cadre et grâce à la coopération du CICTE, la Colombie a déployé des groupes nationaux d'alerte, de vigilance et de prévention qui participent à l'élaboration de stratégies nationales de cybersécurité. De même, elle a participé à des ateliers, des cours et des réunions sur la gestion des incidents liés à la sécurité de l'information et sur les crimes cybernétiques.

Enfin, il faut ajouter que le pays a signé des accords avec des entreprises et des organisations internationales appartenant à l'industrie de l'information et des communications, dont notamment l'accord avec Microsoft visant l'accès à des organismes comme le « Cybercrime Center » et à d'autres programmes de cybersécurité; et l'accord avec le groupe de travail dit « anti-phishing » afin de se joindre à la coalition mondiale d'autorités légales, d'entreprises et d'organismes gouvernementaux qui s'emploient à créer des mécanismes d'alerte et de riposte plus efficaces face aux incidents cybernétiques.

Mesures internationales destinées à renforcer la sécurité de l'information

Le problème de la sécurité ne concerne pas que le Gouvernement, qui ne pourra le résoudre sans le concours d'autres acteurs – l'université, l'industrie et la société civile – pour affronter avec succès les risques liés à l'usage grandissant des technologies de l'information et des communications dans tous les domaines.

Dans ce cadre, la Colombie estime que, pour renforcer mondialement la sécurité de l'information internationale, il importe que la communauté internationale :

- Trouve des mécanismes pour mieux faire comprendre à la société, aux responsables et aux entités de chaque État la nécessité de créer une culture de sécurité de l'information et l'importance de la coopération internationale à la lutte contre la cybercriminalité;
- Affirme que les États sont tenus d'élaborer des stratégies visant à renforcer les capacités nationales de cybersécurité et de cyberdéfense;
- Exhorte les États à identifier leurs infrastructures essentielles et à élaborer un programme destiné à améliorer leur sécurité et leur résilience;
- Encourage l'alignement des cadres normatifs nationaux sur les instruments internationaux de cybersécurité en vigueur. Une meilleure harmonisation normative entre les pays facilite l'établissement de voies de coopération entre eux en matière de prévention, d'enquête et de poursuites visant le cybercrime.

Ce travail d'harmonisation doit prévoir la classification des crimes liés à l'usage des technologies et l'établissement de règles claires sur la juridiction et la compétence judiciaires.

- Promeuve l'établissement, pour les États et les entités nationales publiques et privées, d' obligations concernant la préservation des archives informatiques afin qu'elles puissent être utilisées dans une procédure d'enquête et de poursuites.
- Élabore un glossaire de termes informatiques propres à la cybercriminalité et généralement inconnus des agents du système de justice pénale, afin d'assurer la confidentialité et l'intégrité des systèmes, réseaux et données informatiques.
- Promeuve l'échange des expériences et des pratiques optimales de cyberdéfense et de cybersécurité ainsi que l'établissement de réseaux de formation spécialisée en la matière.
- Exhorte les États à faire partie des réseaux d'alerte aux incidents cybernétiques.

Cuba

[Original : espagnol]
[27 mai 2014]

Cuba partage pleinement la préoccupation qu'exprime la résolution 68/243 concernant l'emploi des technologies et des moyens d'information à des fins susceptibles de nuire à la stabilité et à la sécurité internationales ainsi qu'à l'intégrité des États et à leur sécurité civile et militaire. De même, cette résolution met l'accent sur la nécessité d'empêcher 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. Quelques gouvernements ont même exprimé la possibilité de réagir à ces attaques au moyen d'armes classiques. 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 hostile 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.

Cuba réitère donc sa condamnation de la guerre que le Gouvernement des États-Unis d'Amérique lui fait par la radio et la télévision et qui viole les règles internationales régissant le spectre radioélectrique. Cette agression est menée sans souci du tort qu'elle peut faire à la paix et à la sécurité internationales, créant ainsi des situations dangereuses.

Les émissions illégales de radio et de télévision contre Cuba visent à provoquer l'immigration illégale, à encourager et à susciter la violence, le mépris de l'ordre constitutionnel et la commission d'actes terroristes. Il est illégal d'utiliser

l'information pour compromettre l'ordre interne d'autres États, violer leur souveraineté, et commettre des actes d'immixtion et d'ingérence dans leurs affaires intérieures.

Ces émissions contre Cuba violent les règles internationales de la Constitution de l'Union internationale des télécommunications, dont le préambule reconnaît l'importance croissante des télécommunications pour la sauvegarde de la paix et le développement économique et social de tous les États, et qui a pour but de faciliter les relations pacifiques, la coopération internationale entre les peuples et le développement économique et social grâce au bon fonctionnement des télécommunications.

Chaque jour et 24 heures par jour, le Gouvernement des États-Unis d'Amérique persiste à faire des émissions radiodiffusées par la bande commerciale d'ondes moyennes qui n'est pas sensée desservir d'autres pays. D'autres émetteurs commerciaux offrent leurs services à des organisations anticubaines pour faire des émissions destinées à saboter l'ordre interne et à duper la population cubaine.

Des émissions analogues sont faites par plusieurs de ces organisations, avec l'aval du Gouvernement des États-Unis, par le biais des bandes à ondes courtes.

Entre avril 2013 et avril 2014, le nombre moyen d'heures consacrées à l'émission de messages subversifs contre notre pays a été chaque semaine de 1 909 à 2 070 heures sur 27 fréquences. En septembre et octobre 2013, deux stations américaines qui émettent pour le sud de la Floride et dont les signaux sont reçus dans la zone occidentale et centrale de notre pays ont commencé à émettre des programmes de teneur contre-révolutionnaire.

Les émissions contre Cuba de la radio-télévision Martí par les systèmes de satellites internationaux et nationaux des États-Unis ont persisté.

Par ailleurs, cette année, l'affaire « ZunZuneo » a été révélée : c'était un plan complet du Gouvernement des États-Unis, qui y a consacré des millions de dollars, pour promouvoir la subversion à Cuba par un service de messages sur les réseaux sociaux.

Par ce programme illégal, actif jusqu'en 2012, des données privées sur des usagers cubains, réunies sans leur consentement, ont permis de dresser, à des fins politiques, leur profil par sexe, âge, goûts et affiliations de divers types.

Comme d'autres opérations subversives, ZunZuneo enfreint les lois cubaines et américaines comme la loi CAN-SPAM 108-187 qui, adoptée par le Congrès des États-Unis en décembre 2003, interdit l'envoi de messages commerciaux ou d'autre type sans consentement exprès du destinataire.

Encore une fois, la Constitution de l'Union internationale des télécommunications est violée chaque fois que de tels usages des technologies nouvelles et en particulier des réseaux sociaux portent atteinte aux relations pacifiques et à la coopération internationale par le bon fonctionnement des télécommunications.

Les pratiques nocives des courriers non désirés (spam) ont fait l'objet de plus de 10 recommandations du Bureau de normalisation des télécommunications et constituent une violation de l'article 37 de la Déclaration de principes adoptée au Sommet mondial sur la société de l'information tenu en 2003 à Genève.

Le Gouvernement des États-Unis doit respecter le droit international et les buts et principes de la Charte des Nations Unies et cesser ainsi ses actions illégales et clandestines contre Cuba que réprouvent le peuple cubain et l'opinion publique internationale.

À cet égard, la Communauté des États d'Amérique latine et des Caraïbes (CELAC) a adopté, le 29 avril, un communiqué soulignant que l'usage illicite des nouvelles technologies de l'information et des communications a un effet nocif sur les nations et sur leurs citoyens.

Dans ce communiqué, la CELAC a exprimé son rejet catégorique de l'usage des technologies contraire au droit international et de toutes les actions de ce type. Elle a souligné 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. Elle a réitéré sa volonté d'intensifier les efforts internationaux visant à sauvegarder le cyberespace et à promouvoir son usage exclusif à des fins pacifiques et comme moyen de contribuer au développement économique et social.

Cuba a appuyé la résolution 68/243 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]
[26 mai 2014]

Dans le cadre de la sécurité de l'information et des télécommunications, la force armée d'El Salvador a mis en place un réseau de télécommunications orales et visuelles et de données indépendantes du réseau public afin de protéger toute l'information contre tout agent extérieur qui voudrait y accéder ainsi que contre les attaques cybernétiques.

Géorgie

[Original : anglais]
[30 mai 2014]

Résumé analytique

La cyberguerre menée contre la Géorgie en 2008 a poussé le Gouvernement à placer la protection des infrastructures essentielles du pays au centre de ses préoccupations. Les services publics et les infrastructures essentielles du pays dépendent de plus en plus de l'informatique, ce qui les rend plus vulnérables à la cybercriminalité. En conséquence, le Gouvernement s'est donné pour priorité de protéger adéquatement les infrastructures essentielles des menaces d'attaque électronique.

Les premières cibles des attaques de 2008 ont été les sites Web du Gouvernement et des médias. Ensuite, les attaques se sont étendues à de nombreux autres sites Web gouvernementaux, aux institutions financières géorgiennes, aux

associations professionnelles, aux établissements d'enseignement, à d'autres sites Web des médias et au forum géorgien sur le piratage informatique. Ces attaques visaient à interrompre leur fonctionnement normal. Hormis les deux grandes banques, les cibles visées étaient principalement des organisations qui auraient pu servir à assurer les communications et coordonner les réactions.

Ces faits démontrent que les attaques électroniques visant les infrastructures essentielles du pays, commises par des acteurs étatiques ou privés, peuvent causer des dégâts matériels et des dommages financiers considérables tant au secteur public qu'au secteur privé. C'est pourquoi le Gouvernement géorgien considère que la cybersécurité fait partie intégrante de la politique de sécurité globale du pays, étant donné surtout que la fourniture des services publics dépend de plus en plus des technologies de l'information et des télécommunications.

Face à ces préoccupations, le Conseil national de sécurité et un groupe de travail spécial constitué de différents organismes gouvernementaux ont mis au point au cours de l'année 2011 la Stratégie nationale de cybersécurité, dans le cadre de l'examen de la sécurité nationale. Cette stratégie et le plan d'action qui l'accompagne ont été mis en débat public en mars 2012 et adoptés en janvier 2013.

Par ailleurs, il a été créé en 2010 au sein du Ministère de la justice l'Agence d'échange des données en tant qu'entité centrale chargée d'élaborer et de faire appliquer les directives et solutions relatives à la gouvernance électronique. Une part importante de ses responsabilités est de garantir la sécurité informatique du secteur public et d'entités privées et notamment :

- D'adopter et d'appliquer les normes et directives de sécurité informatique relatives au secteur public et aux infrastructures essentielles;
- De fournir des services de conseil et d'effectuer des évaluations dans le domaine de la sécurité informatique;
- De mener des activités de sensibilisation aux questions de sécurité informatique tant dans le secteur public que le secteur privé;
- De s'acquitter de son mandat en matière de cybersécurité en ayant recours à l'équipe d'intervention nationale en cas d'urgence informatique.

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

Portugal

[Original : anglais]
[20 mai 2014]

Dans sa résolution 68/243 relative à la question susmentionnée, l'Assemblée générale a rappelé le rôle crucial que jouent la science et la technologie dans le contexte de la sécurité internationale, constatant que les innovations scientifiques et techniques peuvent se prêter à des applications civiles aussi bien que militaires et qu'il faut soutenir et encourager les progrès de la science et de la technique. Les progrès informatiques ouvrent de plus en plus de perspectives de développement de la civilisation, de coopération entre les États, de promotion de la créativité et de circulation de l'information dans l'ensemble de la collectivité.

Cependant, ces techniques et moyens peuvent servir à des fins incompatibles avec la stabilité et la sécurité internationales et porter atteinte à l'intégrité des États dans les domaines civil et militaire.

Dans sa résolution 68/243, l'Assemblée générale, rappelant le rapport du Groupe d'experts gouvernementaux (A/68/98), demande aux États Membres de faire part de leurs observations dans quatre domaines :

1. L'ensemble des questions qui se posent en matière de sécurité informatique;

2. Les efforts engagés au niveau national pour renforcer la sécurité informatique et promouvoir la coopération internationale dans ce domaine;

3. Les principes devant permettre de renforcer la sécurité des systèmes télématiques mondiaux;

4. Les mesures que la communauté internationale pourrait prendre pour renforcer la sécurité informatique à l'échelon mondial.

Le rapport du Groupe d'experts gouvernementaux présente certaines recommandations sur les normes, règles et principes de comportement responsable des États, les mesures de confiance et l'échange d'information sur les mesures de renforcement des capacités.

Partant de ces recommandations, on peut d'écrire la situation du Portugal comme suit :

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

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

2. Il amplifie ses efforts pour faire appliquer la législation en matière de sécurité et d'intégrité des réseaux et a notamment mis en place en matière de risque des méthodes 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 sur le fonctionnement des services. Les procédures d'évaluation de la sécurité sont également importantes; elles sont appliquées par le Centre national de notification des violations de la sécurité et des atteintes à l'intégrité;

3. En ce qui concerne la protection des données personnelles et de la confidentialité, des changements sont intervenus; il est notamment devenu obligatoire de signaler les violations des données personnelles;

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

5. 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.

II. Mesures de confiance et échanges d'informations

1. Compte tenu de la mondialisation, il est indispensable d'encourager les échanges d'informations;

2. Les efforts déployés à l'échelon national ont porté essentiellement sur l'exécution d'exercices conjoints auxquels participent le public et des entités privées, la promotion de la normalisation sur le plan technique et l'organisation de conférences et 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 présente des difficultés;

2. Il convient de faciliter l'accès aux connaissances;

3. Le sommet de la hiérarchie n'est pas suffisamment conscient de ses responsabilités dans ces domaines.

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

[Original : anglais]
[29 mai 2014]

Aperçu général

Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord se félicite de pouvoir donner à la résolution 68/243 de l'Assemblée générale, intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », une suite qui amplifie celle donnée en 2013 à la résolution 67/27. Dans sa réponse, 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 termes connexes.

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; celles-ci reposent sur la stratégie nationale pour la cybersécurité du Royaume-Uni, publiée en novembre 2011.

Le Royaume-Uni a participé de manière active et constructive au débat international sur la cybersécurité. Nous avons fourni des experts pour les trois Groupes d'experts gouvernementaux et nous félicitons du rapport consensuel du dernier Groupe, qui 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 affirme que le droit international s'applique au cyberespace. Le Royaume-Uni se félicite également de l'adoption au niveau régional des premières mesures de confiance concernant le cyberespace, qui ont été négociées avec succès à l'OSCE. Sa réponse décrit ses efforts pour promouvoir l'échange des meilleures

pratiques dans le monde entier, tant en collaborant avec ses partenaires internationaux dans la lutte contre la cybercriminalité et le traitement des principaux incidents qu'en cherchant résolument à renforcer les capacités et les aptitudes dans ce domaine.

Le Royaume-Uni attend avec intérêt la poursuite des progrès dans tous ces domaines, notamment en ce qui concerne le prochain Groupe d'experts gouvernementaux, la mise en œuvre des mesures de confiance de l'OSCE et l'élaboration de nouvelles mesures dans la région de l'OSCE ainsi que dans les autres régions, la création d'équipes d'intervention informatique d'urgence coopérant davantage entre elles, le renforcement de la coopération en matière de répression de la cybercriminalité et la promotion d'une approche multipartite.

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 à l'adresse http://www.un.org/disarmament/topics/informationsecurity/.

Serbie

[Original : anglais]
[28 mai 2014]

Compte tenu de la grande importance que revêt la sécurité informatique à l'échelle nationale et mondiale, la République de Serbie a entrepris de prendre des mesures et de mettre en place des mécanismes de sécurité efficaces. Dans la stratégie de développement au niveau national de la société de l'information à l'horizon 2020, qu'elle a adoptée en 2010, elle a rangé la sécurité informatique parmi ses six domaines prioritaires. La Serbie n'a pas de stratégie nationale consacrée à la sécurité informatique, mais traite de ce sujet dans un certain nombre de documents. En octobre 2013, un groupe de travail spécial a été chargé d'élaborer un projet de loi sur la sécurité informatique. Cette loi, qui est calquée sur les cadres juridiques internationaux pertinents dont celui de l'Union européenne, prescrit un dispositif institutionnel de sécurité informatique, des mesures propres à renforcer la sécurité des systèmes télématiques nationaux, notamment ceux des organismes et des entreprises publiques des normes pour la coordination des mesures préventives concernant les risques liés à la sécurité des systèmes télématiques, la création d'une équipe nationale d'intervention informatique d'urgence, les mesures de sécurité spécifiques et les précautions préalables à appliquer en ce qui concerne les systèmes informatiques des organes de l'État, la sécurité des données confidentielles dans les systèmes téléinformatiques, la cryptosécurité et la protection contre les rayonnements électromagnétiques qui compromettent la sécurité.

Le Département de l'informatique de l'administration des services communs des organes de l'État est chargé de la protection de la sécurité informatique et des données et de l'application des normes de sécurité régissant les systèmes informatiques des organes de l'État. Son rapport annuel mentionne que dans le cadre de sa mission de protection des systèmes télématiques des institutions publiques, il

assurait quotidiennement la protection contre les attaques cybernétiques que le réseau subit chaque jour.

Le réseau éducatif et de recherche serbe intervient en cas d'incident lié à la sécurité informatique dans les établissements d'enseignement et de recherche scientifique du pays. Dans son rapport annuel de 2013, il est fait état d'un nombre d'incidents en augmentation par rapport à 2012, la vétusté du matériel étant mentionnée comme l'une des raisons expliquant la recrudescence de ces attaques.

Seule une culture de la sécurité informatique bien assise à tous les niveaux de la société peut renforcer localement la sécurité des systèmes informatiques nationaux. De même, seuls de solides systèmes nationaux de sécurité informatique peuvent contribuer à l'application des principes internationaux de sécurité informatique pour renforcer la sécurité de la télématique au niveau mondial.

Le Bureau du Conseil national de la sécurité et de la protection des données confidentielles est le service gouvernemental chargé de coordonner dans le pays l'application des mesures de sécurité nationales et celles de l'Union européenne. Une partie de ses activités s'est traduite par l'adoption de mesures relatives à l'assurance de l'information et à la coordination de leur application par les organes de l'État et d'autres institutions aux fins de la protection des données confidentielles. Dans ce contexte, un décret relatif aux mesures de protection des données confidentielles des systèmes télématiques a été promulgué en 2011 (Journal officiel de la République de Serbie, n° 53/2011). Au niveau international, le Bureau du Conseil national de la sécurité participe activement depuis 2011 au Forum des directeurs des agences nationales de sécurité des pays de l'Europe du Sud-Est, lequel vise notamment à renforcer l'assurance de l'information et la protection des données confidentielles dans les pays de la région conformément aux normes internationales. Le Bureau du Conseil national de la sécurité remplit les fonctions de coordonnateur principal chargé d'élaborer un modèle régional de défense cybernétique dans le cadre des agences de sécurité des pays de l'Europe du Sud-Est.

Le Bureau du Conseil national de la sécurité a élaboré et envoyé pour examen, harmonisation et approbation aux autres membres du groupe de travail thématique, un certain nombre de recommandations connexes. Celles-ci figurent dans deux documents de travail intitulés « Objectifs du programme de cyberdéfense » et « Questionnaire sur la cyberdéfense des agences nationales de sécurité des pays de l'Europe du Sud-Est ».

Le Ministère de la défense serbe contribue à la mise en œuvre de la résolution 68/243 de l'Assemblée générale. Ses services participent activement au groupe de travail chargé d'élaborer un projet de législation sur la sécurité informatique.

En outre, le Ministère de la défense est en train de constituer divers services dont les activités couvriront la sécurité informatique et la cyberdéfense.

Suisse

[Original : anglais]
[29 mai 2014]

A. Vue d'ensemble des questions relatives à la sécurité informatique

L'informatique et les communications sont devenues un moteur indispensable de l'activité sociale, économique et politique. La Suisse est déterminée à saisir les possibilités qu'offrent ces technologies. Elle prend en compte leur évolution et les problèmes qui leur sont associés pour façonner la société de l'information grâce à la stratégie établie à cet effet par le Conseil fédéral.

Toutefois, l'utilisation de l'informatique et des communications expose les infrastructures correspondantes à des utilisations abusives à caractère criminel, politico-militaire, terroriste ou relevant du renseignement, ou à des dysfonctionnements. Perturbations, manipulations et attaques ciblées menées sur les réseaux électroniques sont autant de dangers qui menacent la société de l'information. Face à cette situation, les États se concertent de plus en plus en matière de cybersécurité aux niveaux régional et international, mus par un sentiment croissant d'insécurité au sujet des vulnérabilités des systèmes informatiques et technologies connexes, et des possibilités de les exploiter à des fins malveillantes.

Ces vulnérabilités et ces menaces existent certes depuis les années 80, mais ce n'est qu'au cours des sept dernières années que l'on s'y est attaqué dans le programme national de sécurité. Le Gouvernement fédéral suisse a ainsi créé en 2010 un groupe d'experts chargé d'analyser les risques et de renforcer la capacité du pays à y faire face.

Pour fonctionner de façon globale, la Suisse dépend d'un nombre croissant d'installations télématiques (ordinateurs et réseaux) reliées entre elles. Cette infrastructure est vulnérable. Des perturbations et attaques de longue durée ou touchant l'ensemble du pays pourraient nuire gravement à son bon fonctionnement technique, économique et administratif. Les attaques peuvent être lancées par de multiples acteurs et pour des motifs divers : individus, militants politiques, organisations criminelles portées à la fraude ou au chantage, et terroristes ou espions à la solde d'un État, dont l'objectif est de perturber et de déstabiliser l'État et la société. Le domaine de l'informatique et les communications constitue une cible de choix non seulement parce qu'il offre de nombreuses possibilités d'usage abusif, de manipulations et de dégradations mais aussi parce qu'il se prête à une utilisation anonyme ne requérant que peu d'efforts. Il est dans l'intérêt national de protéger le pays contre de telles perturbations et attaques. C'est pourquoi nous nous félicitons de la conclusion du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, selon laquelle le droit international s'applique à l'informatique et aux communications.

B. Mesures prises à l'échelle nationale pour renforcer la sécurité informatique et pour favoriser la coopération internationale dans ce domaine

Le 27 juin 2012, le Gouvernement fédéral suisse a adopté la stratégie nationale de protection de la Suisse contre les cyberrisques, jetant ainsi les fondements d'une

démarche générale intégrée pour faire face à ces risques. Cette stratégie vise à améliorer la détection précoce des cyberrisques et des menaces émergentes, à rendre les infrastructures nationales plus résistantes face aux cyberattaques et, d'une manière générale, à réduire ces risques. L'accent est mis sur le cybercrime, l'espionnage et le sabotage. La logique qui sous-tend cette stratégie est la nécessité de créer une culture de la cybersécurité, d'instaurer une responsabilité partagée et d'établir une approche fondée sur les risques. La stratégie prône une meilleure coordination au niveau de l'État et encourage les partenariats entre secteur public et secteur privé et une coopération renforcée sur la scène internationale.

La stratégie comprend un ensemble de 16 mesures qui doivent être mises en œuvre d'ici à 2017. Pour en assurer l'application effective dans les meilleurs délais, le Gouvernement suisse a adopté le 15 mai 2013 un plan détaillé de mise en œuvre. Il a également établi un comité directeur dans lequel sont représentées les institutions désignées pour la mise en œuvre de mesures spécifiques. Ce comité directeur est chargé de veiller à ce que la stratégie soit exécutée de manière coordonnée et adéquate. Ses attributions et responsabilités couvrent la coordination des départements fédéraux[2] compétents et des organismes locaux concernés. Sur le plan opérationnel, le Gouvernement a établi un groupe de coordination qui est censé appuyer les travaux du comité directeur.

Les mesures couvrent des domaines tels que l'analyse des risques et de la vulnérabilité et l'analyse des menaces, la gestion de la continuité des activités et des situations de crise, le renforcement des compétences ou encore la coopération et les initiatives internationales.

Les 16 mesures relèvent de quatre domaines principaux :

– La prévention (analyse des risques, et de la vulnérabilité et état de la menace);

– Les interventions (gestion des incidents, mesures actives et répression);

– La continuité (gestion de la continuité des activités et gestion des crises);

– Les activités d'appui (coopération internationale, enseignement et recherche, fondements juridiques, etc.).

C. Principes visés au paragraphe 2 de la résolution 68/243 de l'Assemblée générale

La coopération internationale est l'un des domaines d'action que la cyberstratégie du Gouvernment suisse doit renforcer. Le pays est résolu à coopérer en matière de politique internationale de la sécurité, pour contrer la menace cybernétique aux côtés des autres pays et des organisations internationales. La Suisse s'emploie résolument à suivre et à orienter l'évolution au niveau diplomatique, et à promouvoir les échanges politiques dans le cadre des conférences internationales et d'autres initiatives diplomatiques.

Dans cette optique, elle participe à divers processus internationaux visant à créer des mécanismes mondiaux. L'OSCE a adopté des mesures de confiance en matière de cybersécurité, auxquelles la Suisse attache une extrême importance. Ainsi, en œuvrant sur deux plans, elle mettra l'accent à la fois sur la mise en œuvre de la première série de mesures de confiance et sur l'élaboration d'autres mesures.

[2] Équivalents de ministères.

Le programme de Londres est un autre processus important auquel la Suisse participe. Enfin, la Suisse qui n'est pas un membre du Groupe d'experts gouvernementaux, s'intéresse aux rapports qu'il produit. À cet égard, nous appuyons en particulier la demande qui vise à poursuivre l'examen des modalités d'application du droit international, et notamment de la Charte des Nations Unies, du droit des droits de l'homme et du droit international humanitaire, à l'utilisation de l'informatique et des communications.

Sur le plan bilatéral, la Suisse tient des consultations politiques régulièrement avec d'autres pays sur les questions relatives au cyberespace.

La Suisse est signataire de la Convention sur la cybercriminalité du Conseil de l'Europe, qui est entrée en vigueur le 1er janvier 2012.

D. Mesures qui pourraient être prises par la communauté internationale en vue de consolider la sécurité informatique à l'échelle mondiale

Il conviendrait de mettre l'accent sur les initiatives et mesures visant à accroître la confiance et à améliorer la compréhension entre les États. Sur le plan bilatéral, les dialogues officiels, semi-officiels et informels entre les États et les autres parties prenantes sur les questions relatives à la cybersécurité se sont révélés fructueux. Il convient d'en organiser davantage.

La sécurité informatique pourrait être renforcée à l'échelle mondiale par la création de mécanismes conjoints propres à éviter une escalade débouchant sur un conflit armé. Ainsi pourrait-on établir des lignes de communication directes tant au niveau technique qu'au niveau politique. La sécurité du cyberespace peut être améliorée par le maintien de contacts réguliers au plus haut niveau.