Nations Unies A/65/154

Assemblée générale

Distr. : générale
20 juillet 2010
Français
Original : anglais/russe/espagnol

Soixante-cinquième session
Point 94 de l'ordre du jour provisoire*
Les progrès de l'informatique et de la télématique et la question de la sécurité internationale

Les progrès de l'informatique et de la télématique et la question de la sécurité internationale

Rapport du Secrétaire général

Table des matières

* A/64/150.

10-45843X (F) 100810 120810

I. Introduction

1. Au paragraphe 3 de sa résolution 64/25, l'Assemblée générale invite tous les États Membres à continuer de communiquer au Secrétaire général leurs vues et observations sur les questions suivantes :

a) Les problèmes généraux en matière de sécurité de l'information;

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

c) La teneur des principes visés au paragraphe 2 ci-dessus;

d) Les mesures qui pourraient être prises par la communauté internationale pour renforcer la sécurité de l'information à l'échelon mondial.

2. Comme suite à cette demande, une note verbale a été adressée aux États membres le 26 février 2010 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

Cuba

[Original : espagnol]
[27 mai 2010]

1. Cuba partage pleinement la préoccupation exprimée dans la résolution 64/25 concernant l'utilisation de la téléinformatique à des fins incompatibles avec la stabilité et la sécurité internationales et pouvant porter atteinte à l'intégrité des États, au détriment de leur sécurité dans les domaines tant civils que militaires. De plus, cette résolution souligne à bon droit la nécessité de prévenir l'utilisation de l'information ou des technologies de l'information à des fins criminelles ou terroristes.

2. Cuba répète que l'usage hostile des télécommunications dans le but déclaré ou secret de compromettre l'ordre juridique et politique des États est une violation des normes internationales dans ce domaine et un emploi négatif et irresponsable de ces moyens, dont les effets peuvent susciter des tensions et des situations nuisibles à la paix et à la sécurité internationales et saper ainsi les buts et principes consacrés dans la Charte des Nations Unies.

3. Cuba attire avec inquiétude l'attention sur le fait que les systèmes informatiques et télématiques peuvent devenir des armes s'ils sont conçus ou employés dans le but de nuire à l'infrastructure d'un État; ils peuvent donc mettre en danger la sécurité et la paix internationales.

4. Cela étant, il y a lieu de répéter la condamnation, déjà émise par la République de Cuba dans divers forums internationaux, de l'escalade agressive des administrations américaines successives dans leur guerre radiotélévisée contre Cuba, violation flagrante des normes internationales qui réglementent le spectre radioélectrique.

5. Le Gouvernement américain n'a pas réparé les dommages qu'il a pu causer à la paix et à la sécurité internationales, en créant des situations dangereuses comme l'usage d'un avion militaire pour transmettre des signaux de télévision vers Cuba, sans son consentement.

6. L'agression radioélectrique contre Cuba à partir du territoire américain contrevient aux principes du droit international qui régissent les relations entre les États ainsi qu'aux normes et règlements de l'Union internationale des télécommunications qui prescrivent la conduite à tenir par les pays membres de cette institution spécialisée des Nations Unies.

7. Chaque semaine, des émetteurs situés sur le territoire des États-Unis diffusent à Cuba des milliers d'heures d'émissions radio et télévisées via 34 différentes fréquences à ondes moyennes, courtes, FM et TV. Au mois de mars 2010, 2 156 heures de transmission illégale ont été comptabilisées par semaine. Plusieurs de ces émetteurs appartiennent ou fournissent leurs services à des organisations liées à des éléments terroristes connus résidant en territoire américain où ils agissent contre Cuba, avec le consentement total des autorités des États-Unis d'Amérique.

8. Les transmissions illégales de radio et de télévision contre Cuba ne diffusent pas d'informations; au contraire, elles les falsifient et les déforment à des fins subversives. Le Congrès des États-Unis d'Amérique vote chaque année un budget de plus de 30 millions de dollars des États-Unis des fonds fédéraux pour financer ce genre d'action. Depuis la création de ces émetteurs, le Gouvernement des États-Unis a dépensé 659,8 millions de dollars des États-Unis à cette fin.

9. Ces émissions provocantes contre Cuba constituent des violations des préceptes internationaux suivants :

– Les principes fondamentaux de l'Union internationale des télécommunications, énoncés dans le préambule de sa Constitution, sur l'importance croissante des télécommunications pour le maintien de la paix et le développement économique et social de tous les États, afin de faciliter les relations pacifiques, la coopération internationale entre les peuples et le développement économique et social par le bon fonctionnement des télécommunications. Le contenu des émissions télévisées transmises par le Gouvernement des États-Unis vers Cuba a un caractère subversif, déstabilisateur et trompeur qui contredit ces principes;

– Les dispositions CS 197 et CS 198 de la Constitution de l'Union internationale des télécommunications, qui précisent que toutes les stations, quel qu'en soit l'objet, doivent être installées et exploitées de manière à ne pas causer de brouillages préjudiciables aux communications ou services de radiocommunication des autres États Membres;

– L'Accord conclu à la neuvième session plénière de la Conférence mondiale des radiocommunications (CMR), qui s'est tenue en novembre 2007, qui indique au paragraphe 6.1, alinéa g) qu'une station de radiodiffusion fonctionnant à bord d'un aéronef et émettant uniquement en direction du territoire d'une autre administration sans l'accord de celle-ci ne peut être considérée comme étant conforme au Règlement des radiocommunications;

– L'article 8, paragraphe 8.3 du Règlement des radiocommunications, qui indique que les fréquences attribuées et inscrites, avec reconnaissance

internationale, doivent être respectées par les autres administrations quand celles-ci effectuent leurs propres attributions afin d'éviter un brouillage préjudiciable;

– L'article 42, paragraphe 42.4 du Règlement des radiocommunications de l'Union internationale des télécommunications, qui interdit aux stations d'aéronefs en mer ou la survolant d'effectuer tout service de radiodiffusion;

– L'avis du Comité du règlement des radiocommunications qui, à sa 35e séance en décembre 2004, a constaté le brouillage préjudiciable aux services cubains que ces transmissions causaient à 213 MHz et a demandé au Gouvernement des États-Unis d'Amérique de prendre les mesures voulues pour l'éliminer. De plus, depuis septembre 2006, ledit comité demande au Gouvernement des États-Unis d'Amérique quelles mesures ont été prises pour éliminer le brouillage à 509 MHz, jusqu'ici sans recevoir de réponse. Le 20 mars 2009, la cinquantième réunion dudit comité a pris fin et, dans son résumé des décisions prises (document RRB09-1/5), elle rappelle encore l'illégalité des transmissions et demande au Gouvernement des États-Unis d'Amérique de prendre toutes les mesures nécessaires afin d'éliminer ces deux cas de brouillage des services de télévision cubains. Lors de sa 53e séance du 26 mars 2010, le Comité du règlement des radiocommunications de l'Union internationale des télécommunications a répété sa conclusion selon laquelle les transmissions des États-Unis d'Amérique provoquent des interférences préjudiciables aux stations cubaines inscrites au Registre international des fréquences et a sommé le Gouvernement des États-Unis d'éliminer cette interférence préjudiciable, de même qu'il a désigné le Bureau qui supervisera la situation et agira conformément aux principes établis dans le Règlement des radiocommunications;

– Le paragraphe 23.3 de l'article 23 du Règlement des radiocommunications de l'Union internationale des télécommunications, qui limite la diffusion d'émissions télévisées hors des frontières nationales.

10. Un rapport de janvier 2009 publié par le General Accounting Office du Gouvernement des États-Unis (GAO) (instance officielle des États-Unis d'Amérique) reconnaît les violations des normes internationales et de la législation interne commises par le programme d'émissions de radio et de télévision du Gouvernement des États-Unis vers Cuba :

– Il montre que l'Union internationale des télécommunications a souligné en 2004 et en 2006 que les émissions télévisées diffusées sur les canaux 13 et 20 causent des interférences préjudiciables aux chaînes cubaines. Le service fédéral n'a entrepris aucune action afin de répondre à la demande de l'Union internationale des télécommunications. De plus, le rapport souligna que la Conférence mondiale des télécommunications, qui s'est tenue en novembre 2007, a indiqué que les transmissions effectuées à partir d'un avion sont contraires à la réglementation de l'Union internationale des télécommunications;

– Il reconnaît que, malgré que les lois des États-Unis d'Amérique interdisent la diffusion nationale de ce type de programmes, tant la télévision que la radio peuvent être captées sur le territoire des États-Unis d'Amérique, principalement à Miami, et que l'utilisation de publicités politiques payantes et

de publicité à caractère sexuel a été détectée sur ces chaînes. De plus, le rapport signale que les programmes vers Cuba ne remplissent pas les standards journalistiques d'équilibre et d'objectivité. On remarque également l'utilisation d'un langage incendiaire et offensif.

11. De plus, Cuba rappelle que la Conférence mondiale des radiocommunications (CMR-07) qui s'est tenue à Genève du 22 octobre au 16 novembre 2007, a adopté des conclusions qui qualifient de non conformes au Règlement des radiocommunications les émissions à partir d'aéronefs depuis les États-Unis vers Cuba. Les conclusions convenues en plénière ont dit textuellement ce qui suit : « Une station de radiodiffusion fonctionnant à bord d'un aéronef et émettant uniquement en direction du territoire d'une autre administration sans l'accord de celle-ci ne peut être considérée comme étant conforme au Règlement des radiocommunications. »

12. Ces conclusions ont été convenues au niveau plénier de la CMR-07 et ont donc force légale pour les travaux de l'Union internationale des télécommunications. C'est ainsi que la Conférence mondiale des radiocommunications a entériné la déclaration faite en 1990 par ce qui était alors appelé le Comité international d'enregistrement des fréquences et selon laquelle les transmissions de télévision à bord d'un aérostat avec des programmes dirigés vers le territoire national cubain contreviennent au Règlement.

13. L'hostilité du Gouvernement des États-Unis d'Amérique envers Cuba s'est manifestée par le blocus économique, commercial et financier imposé depuis près de 50 ans et qui affecte aussi les domaines de l'information et de la télématique :

– Cuba n'a pas le droit d'accéder aux services qu'offrent un grand nombre de sites Web sous prétexte que la liaison émane d'une adresse Internet (IP) relevant du domaine cubain .cu;

– Sans préavis, on a bloqué des domaines .com liés à Cuba, mesure prise récemment par le Bureau du contrôle des avoirs étrangers;

– De par les règles du blocus économique, commercial et financier appliqué à Cuba par le Gouvernement des États-Unis d'Amérique, Cuba ne peut se connecter aux câbles à fibre optique qui entourent l'archipel cubain. Cela oblige le pays à payer pour des services de satellites dont la disponibilité est réduite de par la largeur de bande, ce qui constitue un grave obstacle à l'acquisition des technologies nécessaires et représente des coûts de connexion élevés;

– Internet est utilisé pour diffuser des campagnes de diffamation à l'égard de Cuba, à des fins subversives et de discrétisation du pays.

14. Cette attitude des Etats-Unis sape l'esprit, la volonté et les résultats qui ont prévalu entre les nations du monde entier lorsqu'elles se sont réunies en Suisse et à Tunis pour le Sommet mondial sur la société de l'information (SMSI) en 2003 et en 2005.

15. Ce sommet a exhorté énergiquement les États à adopter, dans la construction de la société de l'information, les dispositions nécessaires pour éviter, et pour s'abstenir d'adopter, toutes mesures unilatérales contraires au droit international et à la Charte des Nations Unies et de nature à nuire au développement économique et

social complet de la population des pays affectés, et à réduire le bien-être de leurs citoyens.

16. L'examen des progrès de l'informatique et de la télématique et de la question de la sécurité internationale par l'Assemblée générale des Nations Unies est très pertinent et chaque jour le rend plus actuel et plus important. Des mesures comme celles que les États-Unis d'Amérique ont prises contre Cuba et dont on vient de parler confirment la nécessité de ce débat et l'urgence de la prise de mesures qui mettront fin à de telles manifestations.

17. Cuba appuie résolument cet exercice à l'Assemblée générale des Nations Unies et continuera de concourir au maximum au développement mondial pacifique de l'informatique et de la télématique et à leur emploi pour le bien de toute l'humanité, et est donc prêt à collaborer avec les autres pays, y compris les États-Unis d'Amérique, pour surmonter les obstacles à la réalisation de ces objectifs.

Grèce

[Original : anglais]
[28 juin 2010]

1. Les problèmes en matière de sécurité de l'information sont traités de manière plus approfondie que par le passé. Une attention particulière est portée aux mesures de lutte contre les menaces modernes, inhérentes à l'avènement de la globalisation des réseaux et des systèmes. Des mesures visant à préserver la libre circulation de l'information sont à l'étude et appliquées au niveau national et au-delà des frontières.

2. Les principes nationaux et internationaux actuels sont suivis et examinés. Il convient de formuler des recommandations internationales dans le cadre de l'évaluation des risques. La problématique de la cybercriminalité doit être traitée. Les droits de souveraineté nationale en matière de sécurité des informations doivent être protégés.

3. Tous les États Membres doivent continuer à faire part au Secrétaire général de leurs points de vue et de leurs observations sur les questions pertinentes. À cet égard, il convient de souligner les points suivants :

a) Toutes les questions en matière de sécurité de l'information sont, en général, hautement appréciées;

b) Des solutions visant à préserver la libre circulation de l'information et à garantir le niveau requis de confidentialité, d'intégrité et de disponibilité sont à l'étude et appliquées au niveau national et au-delà des frontières;

c) Il convient d'élaborer et de définir d'un commun accord des principes d'interconnexion de réseaux offrant des perspectives d'application et de partage au niveau national et international. L'évaluation des risques eu égard à l'interconnexion des réseaux doit revêtir un caractère prioritaire et des lignes directrices internationales pertinentes doivent être formulées. En outre, comme la nécessité de prendre des mesures en faveur de la lutte contre la cybercriminalité constitue une source d'inquiétude importante pour toute nation, il convient de définir des lignes directrices cohérentes au niveau international dans une optique de coopération, d'efficacité et d'économie. Enfin, la nécessité pour une nation de préserver sa

souveraineté et de disposer d'une base d'informations propre doit être prise en compte dans le cadre de l'élaboration de tout principe;

d) Mesures qui pourraient être prises par la communauté internationale pour renforcer la sécurité de l'information à l'échelon mondial :

1) Présentation détaillée et définition commune des principes internationaux pertinents;

2) Proposition d'un plan d'orientation pour une infrastructure globale harmonisée, couvrant les principales questions législatives afin d'offrir à des utilisateurs agréés la sécurité requise en matière d'information dans le cadre de la gestion électronique de la correspondance et de la messagerie, tout en assurant différents moyens de communication;

3) Harmonisation et diffusion des principes adoptés dans le cadre d'alliances multinationales et de groupes de petites nations afin de les appliquer au niveau mondial. La conclusion d'un accord visant à spécifier la menace et ses effets négatifs pourrait avoir une portée plus grande que toute mesure de conception élaborée puisque celle-ci pourrait être exploitée par des personnes malveillantes;

4) Par ailleurs, la souveraineté de la nation doit être comprise comme la référence de base dans le cadre de toute tentative de globalisation. Il convient d'élaborer un principe international pour la définition de passerelles d'échange d'informations, incluant des solutions reflétant le niveau d'intégration souhaité. Il devrait alors servir de guide dans tous les efforts déployés au niveau national, multinational et international.

Mexique

[Original : espagnol]
[18 mai 2010]

Problèmes généraux en matière de sécurité de l'information

1. Les institutions bancaires et financières ainsi que les organes du Gouvernement fédéral traitant de la sécurité publique et de la sécurité nationale sont les organes qui fournissent le plus d'efforts dans le pays en matière de sécurité informatique. Le secrétariat pour la sécurité publique fédérale dispose d'une Unité chargée de la cybercriminalité et d'une Police cybernétique chargée de la cybercriminalité relevant de la sécurité publique.

2. D'autre part, bien que des efforts isolés soient fournis dans le combat contre la cybercriminalité dans les trois branches gouvernementales, il n'existe aucune politique de sécurité cybernétique émanant du Gouvernement fédéral qui guide les stratégies de lutte contre la cybercriminalité dans le pays. La législation en la matière demande à être renforcée, les juges doivent disposer de plus d'instruments leur permettant de traiter et de sanctionner la cybercriminalité. La réglementation pour les fournisseurs de services Internet demande également à être complétée afin que ceux-ci soient tenus de conserver un registre des activités de leur plate-forme et de rapporter des informations relatives à un possible incident. D'autre part, des accords internes ainsi que des accords de coopération avec d'autres pays relatifs à la

cybercriminalité et au cyberterrorisme portant atteinte à la sécurité nationale doivent être conclus.

Les efforts au niveau national et les activités de coopération internationale pour le renforcement de la sécurité de l'information

3. Voici quelques exemples d'efforts engagés au Mexique afin d'assurer la sécurité de l'information :

a) Réglementation de certains cas de cybercriminalité dans les lois suivantes : le Code pénal fédéral, le Code pénal du district fédéral, le Code fédéral de procédure pénale, la Loi su la protection des données de Colima et les Codes pénaux des États d'Aguascalientes, Sinaloa, Tabasco et Tamaulipas;

b) Le 30 avril 2009, le Décret par lequel la section XXIX-O est ajoutée l'article 73 de la Constitution politique des États-Unis du Mexique, qui établit la faculté du Congrès de l'Union à légiférer en matière de protection des données personnelles détenues par des particuliers, a été publié au Journal officiel de la Fédération;

c) Le 1er juin 2009, le Décret qui complétait l'article 16 de la Constitution d'un second paragraphe a été publié. Celui-ci reconnaît que toute personne dispose du droit à la protection de ses données personnelles, à l'accès, la modification et la suppression de celles-ci ainsi que du droit de manifester son opposition, dans les termes prévus par la loi, laquelle établira les exceptions aux principes qui régissent le traitement des données, pour des raisons de sécurité nationale, des dispositions d'ordre publique, de sécurité et de santé publique ou aux fins de protéger les doits de tierces personnes.

d) Le Mexique dispose du CERT de l'UNAM (équipe d'intervention informatique d'urgence de l'Université nationale autonome du Mexique) qui s'occupe des problèmes de sécurité dans le domaine académique et offre une aide et un support technique aux autorités gouvernementales du Mexique dans les affaires de cybercriminalité;

e) La Police fédérale dispose en son sein d'une Police cybernétique chargée de donner suite aux enquêtes sur les délits de sécurité publique.

f) Un rapport relatif à la cybervulnérabilité est en cours de rédaction au sein du Gouvernement fédéral. Il vise à informer les hautes autorités du Gouvernement fédéral des incidents cybernétiques au niveau mondial aux fins de prévisions et d'appui d'initiatives contribuant au renforcement de la cybersécurité au Mexique.

g) Le Gouvernement fédéral est en train de planifier la création d'une CSIRT[1] nationale afin de coordonner les efforts de surveillance de la cybercriminalité au niveau interne et externe;

h) La cybervulnérabilité est reprise dans l'Agenda Nacional de Riesgos (instrument prospectif qui identifie les risques et les menaces pour la sécurité nationale);

[1] CSIRT Computer Security Incident Response Team (Équipe de réponse aux incidents de sécurité informatique).

i) Des programmes de conscientisation du public sont mis en œuvre et coordonnés par des entités publiques et privées afin de prévenir la cybercriminalité;

j) Le Mexique participe à plusieurs forums et conclut des accords de bonne entente en matière de cybercriminalité avec d'autres pays.

Les mesures qui pourraient être prises par la communauté internationale pour renforcer la sécurité de l'information à l'échelon mondial

a) Création de législations adéquates ou mise à jour des législations existantes au besoin pour la protection des informations dans le cyberespace.

b) Formation des juges aux thèmes de la cybersécurité afin qu'ils soient à même de comprendre la nature de la cybercriminalité et de rendre des sentences adéquates.

c) Création de CSIRT nationales afin de coordonner les efforts de surveillance des incidents de sécurité majeurs. Ces CSIRT seraient les points de contact avec les autres pays.

d) Maintenir une communication permanente entre les CSIRT nationales afin de s'organiser en cas d'incident régional ou mondial.

e) Réalisation de forums pour l'échange d'expérience et la formation pour les équipes de sécurité membres de la communauté internationale.

f) Conclusion d'accords internationaux de collaboration dans la lutte contre la cybercriminalité afin d'accélérer les enquêtes et de former un front commun.

Panama

[Original : espagnol]
[21 juin 2010]

1. La République du Panama dispose de plusieurs institutions engagées dans la lutte contre l'utilisation illicite d'Internet à des fins délictueuses, en ce compris les actes terroristes. Parmi ces institutions, on retrouve le Conseil de Sécurité Nationale et l'Institut de médecine légale et des sciences légistes – Département de la criminalité.

2. Le Conseil de Sécurité Nationale est chargé de mener des recherches concernant, notamment, le crime organisé et le terrorisme en cas d'attaque aux biens et à l'intégrité du territoire national.

3. Pour sa part, l'Institut de médecine légale et des sciences légistes dispose du Département de la criminalité qui fut créé par la Loi 69 du 27 décembre 2007. Ce Département effectue des travaux de recherche sur la cybercriminalité.

4. Notre Code pénal classifie, réprime et sanctionne l'utilisation d'Internet à des fins terroristes. Son article 289 stipule que « Toute personne utilisant Internet pour apprendre à fabriquer un engin explosif ou pour recruter des personnes afin de commettre un acte terroriste sera sanctionnée par une peine d'emprisonnement allant de cinq à dix ans ».

5. Il existe d'autres dispositions légales pénalisant l'utilisation d'Internet à des fins délictueuses. Les sanctions peuvent être pénales, civiles ou administratives. Il s'agit de la loi 14 du 18 mai 2007, section VIII, chapitre 1 sur les « Délits contre la sécurité informatique », de la loi 51 du 22 juillet 2008 sur la « Réglementation des documents électroniques, des signatures électroniques et la prestation de services ainsi que l'adoption d'autres dispositions visant au développement du commerce électronique », et de la loi 38 du 8 février 1996 « Par laquelle sont dictées des normes de réglementation des télécommunications en République du Panama ».

Qatar

[Original : anglais]
[25 mai 2010]

1. L'État du Qatar est persuadé que l'utilisation des technologies de l'information et de la communication doit être conforme à la Charte des Nations Unies et aux principes de base des relations internationales. De plus, la libre circulation des informations doit être garantie sans préjudice de la souveraineté nationale tout en préservant la sécurité et le respect des différences culturelles, politiques et morales entre les nations.

2. Les efforts déployés au niveau national reposent sur l'intérêt de la sécurité des communications et la nécessité de l'améliorer ponctuellement afin de suivre la même évolution que celle qu'elle présente aux niveaux national et international.

3. Les efforts nationaux peuvent se résumer comme suit :

– Définir des stratégies et des politiques et promulguer des lois visant à limiter l'utilisation de cette technologie à des fins non conformes aux objectifs de la protection de la stabilité de la sécurité;

– Établir un mécanisme destiné à renforcer la sécurité de l'information afin de garantir la protection de l'infrastructure des informations confidentielles au Qatar;

– Le bureau chargé de la sécurité sur Internet et des renseignements (Office of Internet Security and Intelligence) entend contrôler les réseaux gouvernementaux et nationaux afin de lutter contre tout acte de cybercriminalité à l'encontre de l'État du Qatar;

– Assurer une gestion efficace des incidents liés à Internet et une bonne coordination des efforts visant à les résoudre en vue de garantir la résolution des problèmes Internet une fois qu'ils ont été identifiés, tout en réduisant au maximum le temps d'indisponibilité du système. Dans l'État du Qatar, ces tâches relèvent de l'équipe d'intervention informatique d'urgence (Q-CERT);

– Accroître la sensibilisation et l'exploitation des informations afin d'améliorer le niveau des compétences techniques et des qualifications des employés au sein des institutions qataries;

– Aider les Qataris dans le cadre des questions liées à Internet;

– Suivre l'évolution dans le domaine des sciences technologiques actuelles liées à la sécurité et la sûreté et évaluer les produits techniques, leur sécurité et leur entretien;

– Tisser des relations internationales dans le cadre de la gestion des questions liées à Internet. L'État du Qatar a participé au Forum FIRST (Forum on Incident Response and Security Teams) et au processus « Meridian ».

4. Les mesures qui pourraient être prises par la communauté internationale pour promouvoir la sécurité de l'information au niveau national :

– Les Nations Unies doivent poursuivre le débat et apporter des explications concernant l'utilisation de l'information et de la technologie de communication avec et sans fil dans la guerre électronique et vérifier si les principes existants du droit international offrent un cadre adéquat pour la définition d'un comportement approprié en ligne eu égard aux actes délictueux;

– Créer un comité international ad hoc pour la sécurité des services d'information avec et sans fil et réaliser des études exhaustives à ce sujet;

– L'État du Qatar encourage tous les États Membres à former des équipes chargées de gérer les urgences informatiques au niveau national;

– Faire appel à des institutions spécialisées dans la sécurité dans le domaine de la communication;

– Sensibiliser l'opinion publique à la problématique de la sécurité en organisant des symposiums et des réunions aux niveaux local et international;

– Encourager les États à coopérer afin de lutter contre l'espionnage et la piraterie électronique;

– Recourir à des équipements de cryptage et de sécurité dans le cadre du transfert des informations et des documents de manière sécurisée afin d'en garantir la confidentialité lors de tout échange;

– Mettre à jour les systèmes de protection et organiser régulièrement des ateliers afin de faire le point sur les dernières innovations scientifiques dans le domaine de la sécurité informatique.

Ukraine

[Original : russe]
[25 mai 2010]

Les progrès de l'informatique et de la télématique et la question de la sécurité internationale

1. L'intérêt suscité par les problèmes de sécurité de l'information s'explique par l'importance croissante de l'information dans divers domaines de la vie de la société. L'introduction dans la vie quotidienne de l'État et de la société de techniques d'information de pointe augmente les possibilités d'attaques malveillantes lancées pas des individus ou des milieux criminels contre les systèmes télématiques et les ressources informatiques des organes gouvernementaux et des structures commerciales.

2. La moitié des infractions informatiques enregistrées dans le monde sont liées à l'accès non autorisé à des données électroniques. De plus en plus, ces infractions

sont motivées par l'appât du gain et elles sont de plus en plus destructrices. Le nombre d'infractions perpétrées par des gangs transnationaux augmente.

3. Les infractions informatiques sont signalées avec beaucoup de retard et il devient impossible d'en dresser un tableau complet car les victimes, aussi bien les structures étatiques que les entreprises, s'efforcent de dissimuler les faits, par crainte de perdre leur autorité et ne souhaitent guère afficher les pertes subies et la faiblesse de leur système de protection. Cette absence de publicité fait qu'il demeure impossible d'élaborer les mesures préventives qui devraient être le fondement de tout système de défense de l'information.

4. En règle générale, les infractions informatiques ne sont que la première étape d'une série d'actes criminels revêtant des formes traditionnelles : vol, fraude, extorsion, etc. Ces infractions deviennent chaque jour plus perfectionnées, plus raffinées, plus difficiles à déceler et entraînent des pertes économiques et politiques énormes pour pratiquement tous les pays du monde. De plus, la majorité des experts établissent un lien direct entre la souveraineté de l'État en matière d'information et les questions de sécurité nationale.

5. La lutte contre la délinquance liée aux technologies de l'information soulève de nombreux problèmes d'ordre juridique, les preuves électroniques étant immatérielles et souvent éphémères. La coopération internationale est d'autant plus importante que les problèmes liés à la cybercriminalité sont difficiles à résoudre et, en fin de compte, il importe que tous les États disposent simultanément des moyens juridiques, procéduraux et normatifs nécessaires.

6. Les enquêtes sur les infractions informatiques exigent une coopération entre les services de police de différents États.

7. Dans la pratique, les enquêtes sont menées conjointement. Le Service de sécurité de l'Ukraine participe activement à des opérations conjointes menées par des services de police et des services spécialisés du monde entier engagés dans la lutte contre la pornographie impliquant des enfants, la fraude sur l'Internet et le terrorisme international.

8. Il est également indispensable de combiner les efforts déployés pour continuer à développer la coopération en matière de sécurité de l'information et de défendre les intérêts communs, notamment sur la base d'accords bilatéraux. À notre avis, le problème de la sécurité de l'information ne pourra être réglé que par une coopération effective des structures de différents États, d'autant plus que la base juridique nécessaire existe déjà.

9. En ce qui concerne la lutte qui doit être menée contre la cybercriminalité et le cyberterrorisme, le Service de sécurité de l'Ukraine préconise les contacts avec les organes de maintien de l'ordre et les services spéciaux d'autres pays.

10. Il convient de noter que les cybercriminels s'en prennent bien souvent aux réseaux des établissements d'État et c'est de la qualité des relations établies entre les pays et de l'optimisation des lois nationales que dépend aujourd'hui le succès dans la poursuite et le châtiment des criminels.

11. Étant donné l'expansion continue de la cybercriminalité dans le monde et les liens qui existent entre les gangs de pirates informatiques de différents pays, les frontières nationales n'arrêtent pas la cybercriminalité, il est donc nécessaire de renforcer sans cesse la coopération internationale dans la lutte contre ce fléau.

12. Afin de donner effet aux décisions du Sommet mondial sur la société de l'information (première phase, Genève, 10-12 décembre 2003, deuxième phase, Tunis, 16-18 novembre 2005), l'Ukraine a adopté une loi sur les principes fondamentaux du développement de la société de l'information en Ukraine dans les années 2007-2015, qui donne la priorité à l'intégration dans l'espace mondial de l'information et au développement de la société de l'information. Cette loi prévoit l'amélioration de la sécurité de l'information faisant appel aux technologies de l'information et de la communication les plus récentes.

13. En outre, un plan de développement des télécommunications en Ukraine a été élaboré, prévoyant des mesures organisationnelles et techniques propres à assurer la sécurité dans le fonctionnement de tous les éléments de l'infrastructure des télécommunications en Ukraine. Plus précisément, il s'agit de :

– Constituer et introduire progressivement une base juridique normative assurant la protection technique et cryptographique de l'information, conformément aux normes européennes et internationales;

– Mettre au point des méthodes modernes de protection de l'information à partir de technologies permettant de résoudre les problèmes complexes de la protection de l'information sur les réseaux télématiques;

– Créer un système de saisie légale des informations sur les réseaux de télécommunication, dans les cas prévus par la loi;

– Créer un centre gouvernemental de coordination pour les questions de sécurité des réseaux télématiques et participer à la création de centres gouvernementaux et non gouvernementaux de compétence, capables d'intervenir en cas d'incidents sur les réseaux de télécommunication.

14. La base normative juridique régissant la protection de l'information en Ukraine reprend notamment : la loi sur les fondements de la sécurité nationale en Ukraine, la loi sur l'information, sur la protection de l'information sur les réseaux télématiques (ci-après « la Loi »), les décrets du Président et du Conseil des ministres de l'Ukraine faisant le point de la protection technique de l'information en Ukraine, le règlement assurant la protection des données sur les réseaux télématiques (ci-après « le Règlement »), le dispositif concernant le raccordement aux réseaux mondiaux de transmission de données et divers textes normatifs déposés auprès du Ministère de la justice applicables aux questions du raccordement des systèmes d'information aux réseaux mondiaux, à la délivrance de licences pour diverses activités, et les dispositions relatives à l'évaluation de la production, s'agissant notamment de la protection de l'information.

15. Diverses lois et réglementations stipulent que les données protégées ne peuvent être traitées que sur des réseaux télématiques protégés, c'est-à-dire relevant du Système complexe de protection de l'information, qui est un ensemble unique de mesures juridiques et organisationnelles et de programmes et moyens techniques permettant d'écarter tout risque. De plus, le Système complexe et ses composantes doivent être conformes aux textes normatifs applicables à la protection de l'information.

16. Pour normaliser les spécifications du Système complexe et des différents systèmes d'information en Ukraine, une cinquantaine de textes normatifs à caractère technique ont été rédigés et mis en application, définissant les critères d'évaluation

du degré de protection des données et permettant de classer les réseaux télématiques de manière à déterminer les modalités d'exécution des travaux concernant la protection des données, ainsi que les critères applicables aux systèmes de protection de l'information et au Système complexe, selon la catégorie de réseau télématique, de la portée et du champ d'application de l'information traitée.

17. L'Ukraine s'est également dotée de son propre système national d'évaluation du degré de protection des technologies informatiques. Ce système repose sur un ensemble de documents normatifs régissant la protection de l'information sur les réseaux télématiques contre les accès non autorisés, textes qui sont en harmonie avec les documents analogues des États Membres de l'Union européenne et les normes internationales, notamment ISO-CEI 15408.

18. L'Ukraine a également adopté une série de mesures organisationnelles et techniques visant à prévenir les actes non autorisés visant les réseaux télématiques des organes de l'État, de la police, des douanes et du fisc, des établissements de crédit et de financement, notamment contre les tentatives d'ingérence dans leurs travaux, à l'aide d'Internet.

19. Conformément aux points 10 et 11 de l'article 16 de la Loi ukrainienne sur « le Service public des liaisons spéciales et de la protection des données d'Ukraine » ayant pour but l'amélioration de la coordination des actions des organes gouvernementaux dans la détection des menaces contre les systèmes informatiques, de télécommunication et télématiques et dans l'élimination des conséquences de ces attaques, la mise en œuvre de la coopération internationale dans ce domaine est assurée par l'unité spéciale (CERT-UA) du Service public des liaisons spéciales et de la protection des données d'Ukraine, créée et mise en place par ce dernier.

20. Conformément à la tendance mondiale du développement d'un réseau de structures d'intervention rapide, la Computer Emergency Response Team (CERT – équipes d'intervention informatique d'urgence) se présente comme l'équipe d'intervention informatique d'urgence. La coordination de ces activités est assurée au niveau mondial par l'organisation internationale FIRST (Forum for Incident Response Security Teams), le Forum des équipes de veille et de réponse aux incidents de sécurité informatique.

21. Le 13 juillet 2009, le CERT-UA, l'unité spéciale du Service public des liaisons spéciales et de la protection des données d'Ukraine (www.cert.gov.ua), a reçu le statut de membre à part entière du FIRST (Full Member).

22. Dans le cadre de ses activités en 2009, CERT-UA a traité 461 avis reçus d'équipes d'intervention informatique d'urgence de 30 pays (Australie, Autriche, Belgique, Hongrie, Hollande, Danemark, Israël, Inde, Espagne, Italie, Canada, Chine, Corée, Lituanie, Malaisie, Allemagne, Norvège, Pakistan, Pologne, Portugal, Russie, Roumanie, Arabie Saoudite, USA, Taiwan, Turquie, Finlande, France, Estonie, Japon) concernant des actes non autorisés sur le réseau Internet ukrainien (propagation des programmes nocifs, attaques du type « déni de service distribué » et autres tentatives d'actes non autorisés).

23. Il convient de préciser que des lois et réglementations ont été adoptées, prévoyant la coopération entre les services spécialisés et les forces de l'ordre en vue d'assurer la sécurité de l'information sur les réseaux télématiques et d'accroître l'efficacité du système d'intervention en cas d'action non autorisée visant les ressources en question.

24. Ceci permet aujourd'hui de protéger l'information à tous les niveaux des réseaux télématiques et du Système complexe, quelles que soient la nature et la sensibilité des données traitées et la complexité du réseau. Toutes les demandes essentielles – spécification, projection, mise en application et évaluation de la protection des ressources informatiques en télématique – sont conformes aux normes appliquées par les organes chargés de la sécurité des État Membres des Nations Unies et de l'Union européenne.

25. Aux fins de formation de spécialistes de la sécurité de l'information et de l'informatique, l'Université d'État des technologies de l'information a créé un institut de protection de l'information qui fait partie des structures pédagogiques et scientifiques de l'université.

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

[Original : anglais]
[2 juin 2010]

1. Le Royaume-Uni est heureux de répondre à la Résolution 64/25 des Nations Unies portant sur « Les progrès de l'informatique et de la télématique et la question de la sécurité internationale ».

2. Nous estimons que cette question revêt une importance primordiale pour toute nation, pour son commerce et la protection de ses citoyens et de manière plus générale, pour la sécurité internationale. Le Royaume-Uni a déployé des efforts considérables pour que la toile constitue un espace sécurisé pour toutes les nations et nous accueillons avec enthousiasme les activités internationales dans ce domaine, car il nous apparaît comme essentiel que toutes les nations collaborent ensemble en vue de promouvoir un environnement sûr et robuste au sein du cyberespace.

Problèmes généraux en matière de sécurité de l'information

3. Nous pensons qu'il est essentiel que le monde actuel se dote d'un cyberespace sécurisé. Les citoyens, le commerce, les infrastructures critiques nationales et les gouvernements sont de plus en plus tributaires d'Internet. Tout événement qui influe négativement sur les services Internet au sein d'une nation est susceptible de générer des conséquences néfastes, parfois graves, pour cette nation. Il convient malheureusement d'observer que différents acteurs brandissent la menace, à la fois au sein et en dehors de toute nation, d'altérer le fonctionnement des services Internet ou de les manipuler qu'elle qu'en soit la raison.

Les efforts au niveau national et les activités de coopération pour le renforcement de la sécurité informatique

4. Le Royaume-Uni poursuit ses efforts, aux échelons national et international, visant à promouvoir la sécurité du cyberespace. Au niveau national, nous avons publié en juin 2009 un document intitulé « National Cyber Security Strategy », dont l'objectif est d'étayer les initiatives lancées sur le plan national dans le domaine de la sécurité informatique. Cette stratégie inclut la nécessité de créer deux nouvelles organisations, le Bureau de la cybersécurité (Office of Cyber Security) et le Centre des opérations de cybersécurité (Cyber Security Operations Centre). Depuis leur création, ces organisations n'ont cessé de se développer. Il existe trois équipes

d'intervention informatique d'urgence sous l'égide du Gouvernement britannique, qui proposent également un service dédié aux infrastructures critiques nationales, à l'armée et à d'autres réseaux gouvernementaux. Sur le plan international, nous sommes également actifs dans ce domaine. Notre implication dans le cadre des Nations Unies inclut sa participation dans le Groupe d'experts gouvernementaux des Nations Unies. Nous assurons également la promotion de la résolution des Nations Unies intitulée « Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infrastructures d'information critiques ». Nous sommes membres de plusieurs organisations de l'Union internationale des télécommunications et nous participons aux activités de l'Organisation pour la sécurité et la coopération en Europe. Grâce à notre participation et notre soutien le plus actif, l'Union européenne s'est penchée sur plusieurs initiatives relatives à la protection des infrastructures critiques nationales au sein de l'Union européenne. Nous partageons aussi l'engagement de l'Union européenne pris dans le cadre des activités du Forum régional de l'ASEAN sur la cybersécurité. De la même manière, nous participons à de nombreuses activités au sein de l'OTAN visant à protéger les réseaux de cette organisation. Le Royaume-Uni est depuis longtemps l'une des nations leaders au sein de MERIDIAN (www.meridian2007.org_), de FIRST (Forum for Incident Response and Security Teams, www.first.org) et d'EGC (European Government Cert Group, www.egc-group.org).

5. Vous pouvez télécharger le document intitulé « UK National Cyber Security Strategy » sur le site Web du Cabinet Office, à l'adresse suivante : www.cabinetoffice.gov.uk.

Les mesures qui pourraient être prises par la communauté internationale pour renforcer la sécurité de l'information à l'échelon mondial

6. Nous invitons toutes les nations à mettre sur pied des équipes d'intervention informatique d'urgence. Nous encourageons toutes les nations à promulguer des lois efficaces au niveau national sur la cybercriminalité. Selon nous, bien que les attaques cybernétiques ne soient pas les seules activités malveillantes dans le cyberespace, elles constituent néanmoins la menace la plus courante. Nul doute qu'une réduction des activités criminelles se traduise par un avantage pour tous. Nous estimons que la Convention sur la cybercriminalité organisée par le Conseil de l'Europe constitue un instrument pertinent dans le cadre de la lutte internationale contre les attaques cybernétiques. Nous pensons aussi que la boîte à outils créée par l'Union internationale des télécommunications et promue au sein des Nations Unies représente une base solide pour les nations désireuses d'évaluer leur niveau de préparation dans le traitement des attaques potentielles à l'encontre des infrastructures critiques nationales. Nous encourageons les efforts déployés au sein de nombreux forums visant à promouvoir les meilleures pratiques en matière de sécurité informatique.

Principes internationaux pertinents

7. Le premier principe international est celui du droit international. Un débat important s'est ouvert, notamment lors de conférences via Internet sur l'applicabilité du droit international actuel sur le cyberespace. Le Royaume-Uni s'est penché sur cette question et il apparaît que les principes existants du droit international, à la fois dans le cadre du recours à la force et du droit en cas de conflit armé, fournissent un cadre adéquat permettant de définir et d'analyser l'utilisation du cyberespace dans un contexte d'hostilités.