Nations Unies A/67/167*

Assemblée générale

Distr. générale
23 juillet 2012
Français
Original : anglais, espagnol
et russe

Soixante-septième session
Point 90 de l'ordre du jour provisoire**
Progrès de l'informatique et des télécommunications et sécurité internationale

Progrès de l'informatique et des télécommunications et sécurité internationale

Rapport du Secrétaire général

Table des matières

* Nouveau tirage pour raisons techniques (8 avril 2013).
** A/67/150.

12-43415* (F) 090413 090413

I. Introduction

1. Au paragraphe 3 de sa résolution 66/24, 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/65/201), leurs vues et observations sur les questions suivantes :

a) L'ensemble des problèmes qui se posent 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) Les principes visés au paragraphe 2 de ladite résolution;

d) Les mesures que la communauté internationale pourrait prendre 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 16 février 2012 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

Colombie

[Original : espagnol]
[21 mai 2012]

Il ne fait aucun doute que l'utilisation des technologies de l'information et des communications représente pour nos pays un progrès considérable. Cependant, dans le même temps, l'essor de ces technologies a entraîné celui des actes de malveillance commis au moyen de ces ressources technologiques à l'échelle mondiale, mettant en évidence la nécessité de prendre d'urgence des mesures pour protéger l'État de ces nouvelles menaces.

L'augmentation de la cybercriminalité et le recours aux nouvelles technologies pour créer des menaces informatiques sont des préoccupations auxquelles doivent faire face tous les pays, car ces phénomènes ont des conséquences importantes sur la sécurité de l'information, aussi bien dans la sphère publique que dans la sphère privée, ce par quoi la société civile est elle aussi menacée : il faut donc appliquer de façon stricte les protocoles et politiques de sécurité nécessaires afin de mettre en place des contrôles permettant de protéger de ces nouvelles menaces l'État et ses infrastructures vitales.

C'est dans ce contexte que la Colombie a élaboré en 2005 la norme ISO 27001, conçue comme un système de gestion global définissant la politique, la structure, les procédures, les processus et les ressources nécessaires à la sécurisation de l'information. L'objectif est de faire respecter des normes de qualité comme le code des bonnes pratiques et des objectifs en matière de contrôle présenté dans la

norme ISO 17799, dont l'objectif principal est le respect des trois principes suivants : confidentialité, intégrité et disponibilité :

- Principe de confidentialité : il s'agit d'éviter que l'information ne soit utilisée par des individus ou des processus qui n'ont pas été autorisés à le faire;
- Principe d'intégrité : il s'agit de garantir l'exactitude et l'intégrité de toutes les données importantes pour une organisation;
- Principe de disponibilité : l'information doit être accessible et utilisable dès que les entités autorisées en font la demande.

Les avantages de la norme ISO 27001 sont les suivants :

a) Elle a permis de mettre en place une méthode de gestion de la sécurité de l'information claire et bien structurée;

b) Les risques de perte ou de vol des informations ont été réduits;

c) Les usagers jouissent d'un accès sécurisé à l'information;

d) Les dangers qui menacent l'information et les contrôles visant à assurer sa sécurité font l'objet de mises à jour régulières;

e) La norme prévoit la possibilité de réaliser des audits externes et internes permettant de repérer d'éventuelles défaillances des systèmes de sécurisation de l'information;

f) Elle garantit le respect des lois et règlements relatifs à la gestion de l'information;

g) Elle contribue à rendre la population plus consciente des problèmes touchant à la sécurité informatique.

En complément de cette norme et dans le cadre de son entreprise de modernisation des cadres juridiques et opérationnels dans le domaine de la sécurité de l'information, le Congrès de la République de Colombie a promulgué le 5 janvier 2009 la loi 1273, qui modifie le Code pénal et crée un nouveau bien juridique protégé appelé « Protection de l'information et des données »; cette loi vise notamment à préserver l'ensemble des systèmes utilisant les technologies de l'information et des communications.

Cette loi essentielle se compose de deux chapitres : « Atteintes à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques » et « Délits informatiques et autres infractions ».

Le chapitre 1 définit les infractions suivantes :

- *Accès frauduleux à un système informatique* : Toute personne qui, n'étant pas autorisée à le faire ou s'affranchissant des limites établies par un accord préalable, accède à tout ou partie d'un système informatique protégé ou non par des mesures de sécurité, ou conserve un accès à ce système contre la volonté d'une personne ayant le droit légitime de le lui refuser, est passible d'une peine d'emprisonnement allant de quarante-huit (48) à quatre-vingt-seize (96) mois et d'une amende d'un montant représentant de 100 à 1 000 fois le montant du salaire mensuel minimum en vigueur;
- *Obstruction illicite d'un système informatique ou d'un réseau de télécommunications* : Toute personne qui, sans y être autorisée, entrave le

fonctionnement d'un système informatique ou empêche d'accéder normalement à ce système et aux données informatiques qu'il contient, ou à un réseau de télécommunications, encourt une peine d'emprisonnement allant de quarante-huit (48) à quatre-vingt-seize (96) mois et une amende d'un montant représentant de 100 à 1 000 fois le montant du salaire mensuel minimum en vigueur, si l'infraction commise ne constitue pas un délit passible d'une peine plus sévère;

- *Interception de données informatiques* : Toute personne qui, ne pouvant se prévaloir d'une décision de justice préalable, intercepte des données informatiques à leur source, à leur point de destination ou à l'intérieur d'un système informatique, ou bien les ondes électromagnétiques émises par un système informatique et qui transportent ces données, est passible d'une peine d'emprisonnement comprise entre trente-six (36) et soixante-douze (72) mois;

- *Préjudice informatique* : Toute personne qui, sans être habilitée à le faire, détruit, compromet, efface, détériore, altère ou supprime des données informatiques ou un système de traitement de l'information ou ses parties ou composantes logiques, risque une peine d'emprisonnement pouvant aller de quarante-huit (48) à quatre-vingt-seize (96) mois et une amende d'un montant représentant de 100 à 1 000 fois le montant du salaire mensuel minimum en vigueur;

- *Utilisation de logiciels malveillants* : Toute personne qui, sans être habilitée à le faire, produit, trafique, acquiert, distribue, vend ou expédie des logiciels malveillants ou tout autre programme électronique dangereux, en introduit sur le territoire national ou en fait sortir dudit territoire, encourt une peine d'emprisonnement de quarante-huit (48) à quatre-vingt-seize (96) mois et une amende d'un montant représentant de 100 à 1 000 fois le montant du salaire mensuel minimum en vigueur;

- *Violation des données personnelles* : Toute personne qui, sans être habilitée à le faire, se procure, rassemble, subtilise, offre, vend, échange, envoie, achète, intercepte, divulgue, modifie ou utilise, en vue de son propre profit ou de celui d'un tiers, des codes ou données personnels contenus dans des fichiers, archives, bases de données ou médiums similaires, encourt une peine d'emprisonnement pouvant aller de quarante-huit (48) à quatre-vingt-seize (96) mois et une amende d'un montant représentant de 100 à 1 000 fois le montant du salaire mensuel minimum en vigueur;

- *Usurpation d'identité de sites Internet afin de récupérer des données personnelles* : Toute personne non habilitée qui conçoit, élabore, trafique, vend, exécute, programme ou envoie des pages électroniques, des liens ou des fenêtres « pop up » à des fins illicites, est passible d'une peine d'emprisonnement allant de quarante-huit (48) à quatre-vingt-seize (96) mois et d'une amende d'un montant représentant de 100 à 1 000 fois le montant du salaire mensuel minimum en vigueur, si l'infraction commise ne constitue pas un délit passible d'une peine plus sévère.

Le chapitre 2 de la loi envisage les infractions suivantes :

- *Vol commis par l'intermédiaire d'outils informatiques ou assimilés* : Toute personne qui, contournant les mesures de sécurité informatiques, se rend coupable de l'infraction envisagée à l'article 239 en manipulant un système informatique, un réseau de système électronique ou télématique ou un autre

médium similaire, ou en usurpant l'identité d'un usager pour franchir les systèmes d'authentification et d'autorisation établis, encourt la peine définie à l'article 240 du Code pénal, à savoir, une peine d'emprisonnement pouvant aller de trois (3) à huit (8) ans;

- *Transfert non autorisé d'actifs* : Toute personne qui, en vue d'un profit financier et au moyen d'une manipulation informatique ou d'un artifice similaire, parvient à réaliser au détriment d'une tierce personne un transfert non autorisé d'actifs, quels qu'ils soient, encourt une peine d'emprisonnement comprise entre quarante-huit (48) et cent vingt (120) mois et une amende d'un montant représentant de 200 à 1 500 fois le montant du salaire mensuel minimum en vigueur, si l'infraction commise ne constitue pas un délit passible d'une peine plus sévère. La même sanction sera appliquée à toute personne qui fabriquera, introduira, possédera ou fournira un programme informatique destiné à commettre le délit décrit ci-dessus ou une escroquerie.

Il ne fait pas de doute que la loi 1273 de 2009 représente une avancée cruciale dans la lutte qu'a engagée la Colombie contre les délits informatiques; toutefois, l'essor des différentes catégories et manifestations de la criminalité organisée, et notamment de la criminalité informatique, a obligé la Colombie à mettre en œuvre une stratégie globale de lutte contre la cybercriminalité axée sur la cyberdéfense et la cybersécurité, dans laquelle la coopération entre les diverses entités concernées est primordiale pour atteindre les objectifs définis par la politique de sécurité de l'information.

À cet égard, le Gouvernement colombien a lancé, en juillet dernier, sa politique nationale de cyberdéfense et de cybersécurité, qui repose sur trois piliers consistant à :

- Adopter un cadre institutionnel approprié qui permette de prévenir, coordonner et maîtriser les menaces et les risques qui surgissent et de formuler des recommandations dans le but d'y parer;
- Dispenser une formation spécialisée en matière de sécurité informatique et développer la recherche sur le cyberespace et la cybersécurité;
- Étoffer la législation sur ces questions, promouvoir la coopération internationale et faire en sorte que la Colombie adhère aux divers instruments internationaux;
- Compte tenu des lignes stratégiques susmentionnées, la Colombie a conçu et mis sur pied les quatre institutions suivantes :

  a) La Commission intersectorielle, chargée d'instaurer une vision stratégique de la gestion de l'information et de définir les principes directeurs applicables à la gestion de l'infrastructure technologique, de l'information publique ainsi que de la cyberdéfense et de la cybersécurité;

  b) L'équipe d'intervention informatique d'urgence de Colombie, organisme national compétent pour les questions de cyberdéfense et de cybersécurité;

  c) Le cybercommandement conjoint des forces armées, chargé de prévenir et de contrer toute menace ou attaque cybernétique susceptible de porter atteinte aux valeurs et aux intérêts de la nation;

d) Le Cybercentre de police, chargé de la cybersécurité sur le territoire colombien, qui est un centre d'information, d'appui et de protection contre la cybercriminalité.

Ces institutions permettront à la Colombie de s'acquitter des mandats que lui confère la politique nationale en matière de cyberdéfense et de cybersécurité, ainsi que de mener une lutte intégrée et efficace contre cette nouvelle forme de criminalité qui se propage à grande allure dans le monde d'aujourd'hui.

Cela étant, la Colombie ne s'est pas bornée à élaborer une politique de cyberdéfense et de cybersécurité : elle a mis en place, dans ce contexte, une série d'initiatives importantes, par secteur, qui visent à renforcer la sécurité de l'information. Il s'agit, notamment, des initiatives récapitulées ci-après :

Initiative	*Entité responsable*	*Champ d'application*
Modèle de sécurité de l'information pour la stratégie de gouvernement en ligne	Programme de gouvernement en ligne – Ministère des technologies de l'information et des communications	Le modèle de sécurité renvoie à l'ensemble des politiques stratégiques ayant trait au gouvernement en ligne, telles que la protection des renseignements personnels et la crédibilité et la confiance dans le gouvernement en ligne. Il établit, entre autres éléments clefs de la sécurité de l'information pour les organismes gouvernementaux : a) la disponibilité des informations et des services; b) l'intégrité de l'information et des données; et c) la confidentialité de l'information.
Recommandations destinées au Gouvernement national pour la mise en œuvre d'une stratégie nationale de cybersécurité	Commission de contrôle des communications	Dans ce document, la Commission de contrôle des communications formule à l'adresse du Gouvernement national des recommandations pour la mise au point d'une stratégie nationale de cybersécurité et offre des outils appropriés pour permettre la collaboration et la coopération entre le Gouvernement et le secteur privé, à tous les niveaux; identifie les moyens de décourager la cybercriminalité; recommande l'élaboration et la mise en œuvre de cadres juridiques en matière de cybersécurité qui soient conformes aux normes internationales; formule des recommandations pour la mise sur pied de systèmes qui permettent de réagir aux incidents mettant en jeu la sécurité sur réseaux, notamment par la surveillance, l'analyse et la prise en charge de ces incidents, et propose des lignes

Initiative	*Entité responsable*	*Champ d'application*
		directrices pour la mise en œuvre d'une culture nationale de cybersécurité qui permette d'améliorer la protection des infrastructures d'information essentielles de la Colombie.
Centre colombien de coordination de la sécurité informatique pour fournisseurs de services Internet	Chambre colombienne de l'informatique et des télécommunications	Le Centre colombien de coordination de la sécurité informatique pour fournisseurs de services Internet est en contact direct avec les centres de sécurité de ses filiales, qui sont les plus grands fournisseurs d'accès à Internet de Colombie. Il coordonne le traitement et le règlement des demandes et des plaintes portant sur des problèmes de sécurité informatique.

Cela étant, outre la question des capacités nationales, il convient de mentionner une série de mesures qui devraient être prises, selon la Colombie, au niveau international pour renforcer la sécurité de l'information. Ainsi, il serait bon de :

- Renforcer les voies de communication entre les États Membres de l'ONU, afin de coordonner les efforts consentis pour lutter à l'échelon international contre les infractions touchant à l'information et aux données;
- Concevoir des instruments internationaux et régionaux permettant de définir les comportements répréhensibles qui, dans chaque État, attentent à la cybersécurité et à la cyberdéfense;
- Déterminer et structurer les protocoles de prise en charge des incidents informatiques, dans la perspective d'une mondialisation de la sécurité de l'information;
- Renforcer les activités de prévention et le cadre juridique de la lutte contre les groupes « hacktivistes », en particulier dans les universités et les écoles, afin de dissuader les jeunes de participer à des organisations de ce genre qui menacent le développement normal de l'infrastructure numérique des États;
- Normaliser la législation en mettant l'accent sur la prévention, la prise en charge et le suivi en matière de sécurité de l'information;
- Assurer une convergence et une mise en œuvre des technologies, en mettant l'accent sur l'adoption de pratiques optimales dans le domaine de la gestion de la sécurité de l'information. À cet égard, il importera de se doter de projets d'investissement dans les technologies de pointe et de bénéficier du soutien des gouvernements pour les projets de développement technologique;
- Mettre sur pied des forums d'échange d'informations et de connaissances sur les normes internationales en la matière.

Réglementation de la République de Colombie en matière de sécurité de l'information

Loi/décision	*Sujet*
Loi n° 527 de 1999 sur le commerce électronique	Définit et réglemente l'accès aux messages de données, au commerce électronique et aux signatures numériques ainsi que leur utilisation et, entre autres dispositions, porte création des organismes de certification
Loi n° 599 de 2000	Porte création du Code pénal. Qualifie le délit de violation des communications, instaure la propriété intellectuelle en droit et sanctionne des comportements indirectement liés aux délits informatiques, tels que l'offre, la vente ou l'achat d'instruments permettant d'intercepter des communications privées. Qualifie le délit d'accès illicite à un système informatique comme suit : « article 195. Quiconque accède illicitement à un système informatique protégé par des mesures de sécurité ou s'en sert contre la volonté de la personne habilitée à l'en exclure, est passible d'une amende »
Loi n° 962 de 2005	Édicte des dispositions visant à rationaliser les démarches et procédures administratives tant des organismes et des entités de l'État que des particuliers exerçant des fonctions publiques ou fournissant des services publics. Préconise l'utilisation de moyens technologiques intégrés pour réduire le temps et l'argent nécessaires à l'accomplissement desdites formalités
Loi n° 1150 de 2007	Incorpore les mesures d'efficacité et de transparence prévues dans la loi n° 80 de 1993 et édicte d'autres dispositions d'ordre général sur la passation de contrats intégrant des ressources publiques. Prévoit spécifiquement la possibilité, pour l'administration publique, de délivrer des documents et des actes administratifs et de diffuser des avis par voie électronique et prévoit à cette fin la mise sur pied d'un système électronique sur la passation de marchés publics
Loi n° 1273 de 2009	Porte modification du Code pénal. Instaure, notamment, un nouveau bien juridique protégé appelé « protection de l'information et des données » et prévoit une protection complète des systèmes utilisant les technologies de l'information et des communications
Loi n° 1341 de 2009	Définit, notamment, les principes et les concepts afférents à la société de l'information et à l'organisation des technologies de l'information et des communications et porte création de l'Agence nationale du spectre

Loi/décision	*Sujet*
Décision n° 2258 de 2009 de la Commission de contrôle des communications	Garantit la sécurité des réseaux des fournisseurs de réseaux et de services de télécommunication. Porte modification des articles 22 et 23 de la décision CRT 1732 de 2007 et des articles 1.8 et 2.4 de la décision CRT 1740 de 2007. Consacre l'obligation, pour les fournisseurs de réseaux ou de services de télécommunication offrant un accès à Internet, de mettre en œuvre des modèles de sécurité, en fonction des caractéristiques et des besoins de leur réseau, afin d'aider à améliorer la sécurité de leurs réseaux d'accès, conformément aux cadres de sécurité définis par l'Union internationale des télécommunications, dans le respect des principes de confidentialité et d'intégrité des données et de disponibilité des éléments du réseau, de l'information, des services et des applications, ainsi que des mesures applicables à l'authentification, à l'accès et à la protection contre l'exclusion. Définit également les conditions requises des fournisseurs de réseaux et de services de télécommunication concernant l'inviolabilité des communications et la sécurité de l'information
Lettre circulaire n° 052 de 2007 (Surintendance financière de Colombie)	Définit les conditions minimales de sécurité et de qualité applicables à la gestion de l'information par le biais de canaux de distribution de produits et de services destinés aux clients et aux utilisateurs

Cuba

[Original : espagnol]
[21 mai 2012]

L'utilisation malintentionnée des télécommunications, avec pour objectif déclaré ou non de porter atteinte à l'ordre juridique et politique des États, constitue une violation des principes reconnus en la matière sur le plan international et peut avoir pour effet de provoquer des tensions et des situations mettant en péril la paix et la sécurité internationales.

Cuba partage sans réserve la préoccupation exprimée par l'Assemblée générale dans sa résolution 66/24 quant au fait que les technologies et moyens informatiques risquent d'être utilisés à des fins incompatibles avec le maintien de la stabilité et de la sécurité internationales et de porter atteinte à l'intégrité de l'infrastructure des États, nuisant ainsi à leur sécurité dans les domaines tant civil que militaire. Cette résolution souligne aussi à juste titre qu'il est indispensable de prévenir l'utilisation de l'information et de l'informatique à des fins criminelles ou terroristes.

À cet égard, la République de Cuba condamne une nouvelle fois la guerre toujours plus agressive menée contre elle par le Gouvernement des États-Unis dans le domaine de l'audiovisuel, en violation de la réglementation internationale du spectre radioélectrique. Les États-Unis se livrent à cette agression sans se soucier de ses retombées éventuelles sur la paix et la sécurité internationales et créent des

situations dangereuses, notamment lorsqu'ils utilisent un avion militaire pour émettre des signaux de télévision en direction du territoire de la République de Cuba sans son consentement.

En 2011, le nombre d'heures d'émissions hebdomadaires illégales diffusées, sur 30 fréquences, depuis le territoire des États-Unis et destinées à Cuba, s'est élevé à 2 193. Certains émetteurs radio, qui sont aux mains ou au service d'organisations liées à des éléments terroristes connus vivant sur le territoire des Etats-Unis, et y menant des activités anticubaines, diffusent des émissions incitant au sabotage, aux attentats politiques et au meurtre de personnalités et traitant d'autres sujets de prédilection du terrorisme des ondes.

La diffusion de ces émissions provocatrices hostiles à Cuba est contraire aux principes internationaux suivants :

- Les grands principes de l'Union internationale des télécommunications, énoncés dans le préambule de sa constitution. Le contenu des émissions télévisées diffusées à Cuba par le Gouvernement des États-Unis a un caractère subversif, déstabilisateur et trompeur, contraire à 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 que soit leur objet, doivent être établies et exploitées de manière à ne pas causer de brouillages préjudiciables aux communications ou services radioélectriques des autres membres;
- Le procès-verbal de la 9e séance plénière de la Conférence mondiale des radiocommunications, tenue en novembre 2007, où il est indiqué, à l'alinéa g) du paragraphe 6.1, « 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 »;
- Le paragraphe 3 de l'article 8 du Règlement des radiocommunications, selon lequel toute fréquence assignée, inscrite dans le fichier de référence et internationalement reconnue, doit être prise en compte par les autres administrations lorsqu'elles font leurs propres assignations afin d'éviter les brouillages préjudiciables;
- Le paragraphe 4 de l'article 42 du Règlement des radiocommunications, qui interdit aux stations d'aéronef en mer ou au-dessus de la mer d'effectuer un service de radiodiffusion;
- L'avis du Comité du Règlement des radiocommunications (RRB) qui, à sa trente-cinquième réunion en décembre 2004, a constaté que les émissions sur la fréquence à 213 MHz se traduisaient par des brouillages préjudiciables aux services cubains et demandé au Gouvernement des États-Unis d'Amérique de prendre les mesures nécessaires pour faire cesser ces émissions. De plus, depuis septembre 2006, le Comité demande vainement à ce dernier de lui indiquer quelles mesures il a prises pour éliminer le brouillage sur la fréquence 509 MHz. Le 20 mars 2009, à l'issue de sa cinquantième réunion, le Comité a publié un relevé des décisions (document RRB09-1/5) dans lequel il réaffirme une fois encore l'illégalité des transmissions et demande au Gouvernement des États-Unis d'Amérique de prendre toutes les mesures nécessaires en vue d'éliminer ces brouillages préjudiciables aux services de télévision cubains;

- Le paragraphe 3 de l'article 23 du Règlement des radiocommunications, selon lequel les émissions de signaux de télévision ne doivent pas dépasser les frontières nationales. Dans un rapport de janvier 2009, l'organisme public d'audit des États-Unis a reconnu que le programme d'émissions de radio et de télévision anticubaines du Gouvernement des États-Unis violait les normes internationales et la législation interne.

La Conférence mondiale des radiocommunications (CMR-07), tenue à Genève en 2007, a adopté des conclusions dans lesquelles elle considère comme non conformes au Règlement des radiocommunications les transmissions des États-Unis vers Cuba à partir d'aéronefs. Le texte adopté en séance plénière établit en effet 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.

En adoptant ces conclusions, qui ont une valeur juridique pour les travaux de l'UIT, la Conférence mondiale des radiocommunications a fait sienne la déclaration de 1990 du Comité international d'enregistrement des fréquences, selon laquelle la transmission de signaux de télévision à partir d'un aérostat en direction du territoire national cubain était contraire au Règlement.

Par ailleurs, le Comité du Règlement des radiocommunications, à sa cinquante-quatrième réunion, tenue en juillet 2010, après avoir examiné dans le détail le rapport du Directeur ainsi que la communication soumise par Cuba [document RRB10-2/3 (Add.1)], a constaté avec regret que le brouillage des émissions diffusées par les stations de radiodiffusion cubaines par des transmissions en provenance des États-Unis se poursuivait et il a décidé de maintenir ses décisions antérieures sur cette question.

En outre, le Comité a pris note de la demande qui lui avait été adressée par « le Bureau, en sa qualité de Secrétaire exécutif du Comité », pour qu'il soumette à la prochaine Conférence de plénipotentiaires la question du brouillage préjudiciable des émissions diffusées par les stations de radiodiffusion cubaines dans les bandes d'ondes métriques et décimétriques. Reconnaissant le droit souverain de chaque gouvernement de soumettre toute question à la Conférence de plénipotentiaires, le Comité a confirmé que les deux représentants du Comité du Règlement des radiocommunications à la Conférence de plénipotentiaires de 2010 et le Secrétaire exécutif du Comité seraient prêts à fournir tous les renseignements et conseils pertinents qui pourraient être nécessaires à la prochaine Conférence de plénipotentiaires.

Plus récemment, en février 2012, la Conférence mondiale des radiocommunications a demandé au Directeur du Bureau des radiocommunications de l'UIT de veiller à l'application de ses décisions et de faire rapport à la prochaine conférence qui se tiendra en 2015, sur le brouillage par le Gouvernement des États-Unis des émissions de radio et de télévision cubaines, qui constitue un acte d'agression perpétré au moyen de la radio et de la télévision.

La Conférence a ainsi confirmé la validité des conclusions qu'elle avait adoptées à sa précédente session, dans lesquelles elle reconnaissait l'illégalité de la transmission par le Gouvernement des États-Unis, au moyen d'aéronefs, d'émissions radiotélévisées anticubaines.

L'hostilité du Gouvernement des États-Unis envers Cuba s'est aussi manifestée par le blocus économique, commercial et financier imposé depuis plus de 50 ans, qui s'étend aux domaines de l'information et des télécommunications :

- Le blocus a lourdement pesé sur le secteur de l'informatique et des communications, lui coûtant 7 396 394 dollars au total en 2010 et 2011;
- Cuba n'a toujours pas le droit d'accéder aux services qu'offrent un grand nombre de sites Web; l'accès est en effet refusé dès lors que l'adresse IP est identifiée comme appartenant au domaine cubain « .cu »;
- Avec un cynisme absolu et une hypocrisie totale, les États-Unis continuent d'accuser à tort Cuba d'interdire à ses citoyens l'accès au réseau mondial, alors qu'en réalité ce sont les dispositions du blocus imposé par les États-Unis qui empêchent Cuba de se connecter au réseau de fibres optiques entourant l'archipel et l'obligent à payer de coûteux services satellitaires;
- Le 6 octobre 2010, le réseau social Twitter a reconnu qu'il était pleinement responsable d'avoir interdit l'envoi de messages émanant des téléphones portables cubains. De plus, il a été découvert en avril 2011 que certaines fonctionnalités n'étaient pas disponibles depuis Cuba, au motif qu'il s'agissait d'un pays « interdit »;
- En février 2011, l'établissement financier Syniverse a cessé de verser à la société cubaine de télécommunications ETECSA les paiements dus au titre des services de téléphonie mobile fournis aux abonnés itinérants, prétextant que sa banque ne pouvait pas effectuer de transactions financières avec Cuba, d'où une perte de plus de 2,6 millions de dollars, venant s'ajouter aux difficultés découlant de cette situation.

L'examen par l'Assemblée générale des Nations Unies des progrès accomplis dans les domaines de l'information et des télécommunications sur le plan de la sécurité internationale est parfaitement pertinent et on ne peut plus important. Des agissements tels que ceux, mentionnés plus haut, des États-Unis contre Cuba confirment qu'il est indispensable de tenir ce débat et urgent de prendre des mesures pour en finir avec cette situation.

Cuba a soutenu la résolution 66/24 de l'Assemblée générale et continuera de faire tout son possible pour permettre l'essor pacifique des technologies de l'information et des télécommunications partout dans le monde, au bénéfice de l'humanité tout entière.

Panama

[Original : espagnol]
[10 juillet 2012]

Les économies du XXI^{e} siècle s'appuient principalement, et toujours davantage, sur le secteur des services, en particulier dans le monde développé. Le commerce électronique n'est jamais que l'évolution la plus récente de ce secteur de l'économie, facilitant les transactions commerciales et réduisant les coûts et délais de livraison des marchandises et des services dans le monde entier. La gouvernance électronique, version étatique du commerce électronique, permet quant à elle aux

États de répondre rapidement et efficacement, grâce à différentes technologies (Web et mobiles), aux nombreuses demandes émanant de leurs citoyens.

Compte tenu de l'usage intensif qui est fait des technologies de l'information et des communications à l'appui du commerce et de la gouvernance électroniques, il convient de faire en sorte que ces technologies répondent aux critères minimaux de confidentialité, d'intégrité et de disponibilité que sont en droit d'attendre les clients et les citoyens d'un État. Une grande partie des efforts déployés aujourd'hui consistent toutefois à apporter des solutions techniques à des problèmes globaux par le biais d'approches multiples.

Nous estimons que l'élaboration de cadres juridiques se fondant sur des normes internationales préalablement adoptées par d'autres États et largement appliquées doit être l'objectif premier des États qui souhaitent promouvoir le commerce et la gouvernance électroniques tout en les protégeant des délinquants et terroristes qui voudraient les exploiter pour mener à bien leurs activités. La création de conditions propices au commerce et à la gouvernance électroniques ne saurait profiter qu'aux économies des pays ayant pris des mesures de protection juridique et technique dans ce domaine.

Il faut également continuer d'œuvrer à la mise au point de techniques et de politiques de défense du cyberespace des États, où se rejoignent les intérêts des différents pays, au moyen de stratégies nationales de cybersécurité susceptibles d'être appliquées dans des délais bien définis et réalistes. Ces stratégies doivent avoir pour objectif de garantir la sécurité et la stabilité nationales et de contribuer à la paix internationale.

Les mesures adoptées par le Panama au niveau national pour renforcer la sécurité de l'information et faciliter la coopération internationale sont les suivantes :

a) Création du Centre national de prise en charge des incidents, par le décret exécutif n° 709 du 26 septembre 2011;

b) Révision du droit substantiel (Code pénal) en vue d'y inscrire de nouveaux délits relevant de la cybercriminalité, puis présentation de cette révision à l'Assemblée nationale pour approbation (projet de loi n° 377);

c) Examen et révision du code de procédure pénale, pour qu'il y soit tenu compte des nouveaux délits figurant dans le Code pénal;

d) Constitution du groupe de travail chargé d'examiner, sous la direction conjointe de l'Autorité nationale pour l'innovation gouvernementale et de l'Autorité nationale des services publics, la responsabilité des fournisseurs d'accès à Internet en ce qui concerne la sécurité de l'information et évaluation de la mise en œuvre des recommandations de ce groupe au niveau régional (Commission technique des télécommunications d'Amérique centrale/Union internationale des télécommunications) par les autorités nationales de tutelle de la région de l'Amérique centrale;

e) Réunion du groupe de travail sur l'exploitation des preuves numériques, sous la direction du ministère public et avec la participation de l'Autorité nationale pour l'innovation gouvernementale;

f) Officialisation de la demande d'assistance technique adressée à l'Organisation des États américains (OEA), pour l'élaboration de la stratégie nationale de cybersécurité;

g) Formation avancée à la gestion des incidents, dispensée en avril au Panama par l'OEA et le Centre de coordination de l'Équipe d'intervention informatique d'urgence;

h) Évaluation de la proposition du Bureau des Nations Unies pour le développement concernant un programme de renforcement des capacités du Panama en matière de lutte contre la cybercriminalité;

i) Participation régulière aux réunions des ministres de la justice et autres ministres, des procureurs généraux des Amériques et des membres du Comité interaméricain contre le terrorisme (relevant de l'OEA);

j) Demande officielle d'adhésion à la Convention de Budapest sur la cybercriminalité, par l'intermédiaire de la note du 31 janvier 2012, adressée à Carlos Arosemena, Ambassadeur du Panama à Bruxelles, par le Ministre des relations extérieures.

S'agissant des mesures que la communauté internationale pourrait adopter en vue de renforcer la sécurité de l'information à l'échelle mondiale, nous estimons qu'il conviendrait d'examiner les recommandations suivantes :

a) Adoption d'un cadre juridique commun qui permette une collaboration entre États à la faveur d'une assistance mutuelle et diligente, en vertu de procédures internationales convenues;

b) Mise au point de stratégies nationales et régionales de cybersécurité;

c) Promotion systématique de l'échange de renseignements entre États par l'intermédiaire des centres nationaux de prise en charge des incidents, dans le but de faciliter la circulation de l'information, en particulier en ce qui concerne la lutte contre la criminalité et le terrorisme;

d) Élaboration de programmes de sensibilisation aux normes locales et internationales applicables à chaque État.

Qatar

[Original : anglais]
[18 mai 2012]

Les initiatives de l'État du Qatar en matière de sécurité de l'information sont fondées sur une approche holistique portant à la fois sur la sécurité des ressources et sur celle des individus qui utilisent ces ressources. La stratégie est conforme aux objectifs du programme qatarien « Vision 2030 », qui met l'accent sur les aspects humains, sociaux et économiques du développement et repose sur des initiatives internationales telles que le Programme mondial de cybersécurité de l'UIT et les principes du Groupe des Huit en matière de protection des infrastructures informatiques critiques.

Actuellement, le programme national de cybersécurité du Qatar (équipe d'intervention informatique d'urgence du Qatar, initiative du Centre d'excellence pour la sécurité de l'information), organisation parrainée par le Gouvernement et placée sous les auspices du Conseil suprême des technologies de l'information et des communications, constitue l'une des pierres angulaires du plan d'action qatarien

sur la cybersécurité, qui comprend la protection des infrastructures d'information critiques et la mise sur pied des services gouvernementaux s'en chargeant.

L'équipe d'intervention informatique d'urgence du Qatar collabore avec des organismes publics, des organisations des secteurs privé et public et des citoyens qatariens afin de surveiller les menaces informatiques et de limiter les risques y relatifs. Parmi ses pratiques établies d'enquête sur les menaces figurent l'expertise judiciaire de pointe en informatique, l'analyse des logiciels malveillants et le suivi des menaces, ainsi que la mise en place de moyens visant à renforcer la préparation aux problèmes de sécurité et améliorer les interventions s'imposant pour les résoudre par l'intermédiaire de programmes de formation en situation. On trouvera ci-après une brève description de ses fonctions.

Collecte de renseignements sur les menaces

Centre des opérations de sécurité. Des analystes spécialisés dans la sécurité utiliseront des outils mis au point en interne (système de suivi des menaces) pour adresser des alertes préventives aux organismes publics et aux organisations d'intérêt critique au sujet des menaces détectées et des outils à utiliser pour les éliminer.

Système de suivi des menaces. Il s'agit d'un système conçu en interne qui permet de compiler et d'analyser les renseignements recueillis sur les menaces auprès de différentes sources afin de limiter l'impact des ordinateurs ou sites Web locaux infectés.

Laboratoire d'analyse des logiciels malveillants

Le laboratoire a pour objectif d'évaluer et d'analyser les menaces constituées par les logiciels malveillants et de s'en prémunir au niveau national. Il œuvre actuellement à l'élaboration d'un rapport détaillé sur le comportement des logiciels malveillants dans les machines infectées; les types de systèmes pris pour cibles; les sources de logiciels malveillants en fonction du pays; et toute connexion Internet avec le serveur de commande et de contrôle. Il contribue également à déterminer la portée des logiciels malveillants identifiés afin d'évaluer le risque associé à la menace qu'ils représentent sur le plan quantitatif et à assurer leur détection en se servant de tous les antivirus existant sur le marché.

Prise en charge publique des incidents

L'équipe d'intervention informatique d'urgence du Qatar se propose de réduire au minimum le nombre de machine infectées dans le pays en apportant l'appui indispensable au secteur public et autres secteurs concernés. Pour atteindre cet objectif et donner les orientations qui conviennent, le Qatar a étendu le champ d'action de son service de prise en charge des incidents aux utilisateurs de connexions Internet personnelles par liaison numérique à débit asymétrique (RNA) via le portail public de prise en charge des incidents. L'équipe d'intervention indique la marche à suivre, donne des conseils généraux et fournit un logiciel de base pour analyser les machines personnelles connectées par RNA et les désinfecter si nécessaire.

Formation à la cybersécurité

L'équipe d'intervention informatique d'urgence du Qatar dispense des cours de formation et organise des ateliers dans le domaine de la cybersécurité à l'intention des spécialistes de l'informatique des organismes publics et d'autres pays membres du Conseil de coopération du Golfe.

Sensibilisation à la cybersécurité

L'équipe d'intervention informatique d'urgence du Qatar pose les bases d'une bonne compréhension des problèmes qui se posent et des pratiques optimales à adopter en matière de cybersécurité, en se concentrant sur les employés des entités publiques et du secteur privé.

Elle œuvre à la protection des infrastructures essentielles, de nombreux secteurs d'activité tels que la finance, l'énergie et les technologies de l'information et des communications revêtant une importance capitale pour l'économie, la population et le Gouvernement qatariens. Elle s'efforce dans ce cadre de protéger les systèmes informatiques qui forment la colonne vertébrale de ces secteurs essentiels, en prenant les mesures suivantes :

- Élaboration à l'échelle nationale de stratégies de protection, de cadres de référence pour les pratiques optimales et d'outils adaptés, et sensibilisation des parties concernées;
- Assistance directe aux propriétaires et exploitants d'infrastructures critiques aux fins d'améliorer leurs dispositifs de défense des systèmes de surveillance et d'acquisition de données (SCADA);
- Analyse des difficultés rencontrées par les différents secteurs d'activité, y compris les dépendances intersectorielles, et mise en œuvre des stratégies de protection adaptées à chaque secteur;
- Collaboration avec les organismes internationaux de protection des infrastructures informatiques afin de définir des solutions transnationales;
- Évaluation du degré de maturité des organismes de protection des infrastructures informatiques dans le pays et suivi des progrès accomplis.

En outre, les responsables du programme de cybersécurité du Conseil suprême des technologies de l'information et des communications poursuivent leur coopération avec le pouvoir législatif pour élaborer diverses lois et normes en vue d'améliorer constamment les moyens dont la nation dispose face aux nouvelles menaces informatiques.

Le Conseil suprême recommande l'adoption et la mise en œuvre, par l'intermédiaire de la communauté internationale, des mesures suivantes :

- Élaboration de cadres juridiques internationaux harmonisés au niveau régional dans tous les pays, dans un délai de cinq ans;
- Création d'une équipe de prise en charge des incidents informatiques dans tous les pays qui n'en disposent pas, dans un délai de trois ans;
- Élaboration de stratégies nationales de cybersécurité, compatibles avec les principes de la coopération internationale, y compris pour la protection des infrastructures informatiques critiques, dans un délai de cinq ans;

- Mise au point de programmes d'enseignement dans le domaine de la cybersécurité, en vue de renforcer les capacités et de favoriser la prise de conscience de divers groupes d'intérêts (gouvernements, milieu universitaire, secteur privé, écoles, notamment);
- Mise en évidence de l'importance des programmes de sensibilisation à la sécurité des enfants et des jeunes dans l'univers numérique.

Turquie

[Original : anglais]
[31 mai 2012]

Les technologies de l'information et des communications envahissent rapidement la vie privée et la vie professionnelle. Des données essentielles pour les particuliers, les institutions ou les gouvernements sont stockées numériquement et transmises à travers le cyberespace. Malgré leurs avantages, les technologies comportent des risques car elles sont incapables de préserver la confidentialité et l'intégrité des données stockées numériquement ou d'assurer la disponibilité des systèmes informatiques. Ces risques peuvent devenir réalité lorsqu'il existe des points faibles dans les systèmes d'information et de communications, imputables à des défauts dans la conception, la configuration ou l'exploitation, ou lorsque les employés et les utilisateurs n'ont pas les aptitudes techniques suffisantes ou sont peu formés ou sensibilisés à la sécurité.

Pour éviter ou limiter ces risques et remédier aux failles, des efforts de plus en plus importants sont déployés en vue de renforcer la sécurité informatique aux niveaux national et institutionnel. Il est jugé essentiel, dans ce contexte, de renforcer les capacités techniques et administratives des cadres, des employés et des utilisateurs des institutions publiques ou privées, ainsi que de les sensibiliser davantage à la sécurité.

Les cadres supérieurs du Gouvernement turc sont dûment sensibilisés à la nécessité d'accroître la sécurité de l'information à l'échelle nationale. En outre, l'Office turc de l'information et des communications axe tout particulièrement ses travaux sur la recherche de pratiques optimales et l'étude des nouvelles menaces présentes dans le cyberespace et s'emploie à organiser et à mener des exercices sur la cybersécurité à l'échelle nationale, à renforcer les capacités nécessaires sur le plan institutionnel et technique pour répondre aux situations d'urgence et à procéder régulièrement à des audits des opérateurs de communications électroniques de façon à veiller à la mise en place de politiques, mécanismes, programmes et mesures de contrôle adéquats permettant de gérer correctement les incidents mettant en jeu la sécurité desdites communications.

Les recherches portant sur les approches internationales adoptées face aux menaces mondiales, les points faibles des systèmes informatiques et les pratiques optimales s'agissant des mécanismes d'information ainsi que la mise en commun des connaissances spécialisées avec d'autres organisations internationales sont jugées utiles pour renforcer la sécurité des systèmes d'information et de télécommunications mondiaux.

Des conventions multilatérales consacrées à la coopération dans le domaine de la lutte contre les incidents mettant en jeu la sécurité de l'information et des

communications dans le cyberespace, ou à l'étude desdits incidents d'un point de vue criminalistique, ainsi que la diffusion d'informations relatives aux bases de données sur les logiciels malveillants, pourraient permettre de renforcer la sécurité informatique à l'échelle planétaire.

Ukraine

[Original : russe]
[31 mai 2012]

L'ensemble des problèmes qui se posent en matière de sécurité de l'information

Du fait du rapide essor des technologies de l'information et de la communication dans tous les domaines de la vie et de la mondialisation des relations informatiques, les activités illégales tendent, dans le monde entier, à investir l'espace virtuel. Aujourd'hui, ne connaissant pas de frontières, la criminalité informatique (ou cybercriminalité) menace les droits et les libertés des citoyens et porte atteinte aux intérêts nationaux et à la sécurité des États.

Ces dernières années, on a enregistré une croissance soutenue du nombre d'attaques informatiques contre de grandes infrastructures nationales, qui ont porté préjudice aux États concernés en altérant des informations importantes et perturbant le fonctionnement d'usines et d'équipements collectifs, les transports et l'approvisionnement en énergie.

Une analyse de l'état de la cybercriminalité en 2011 dans les États où les systèmes d'information d'institutions et d'organes publics ont été victimes d'actes de piratage ayant entraîné de réelles perturbations révèle l'ampleur des risques pour la société et le caractère imprévisible des conséquences des cyberattaques.

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

S'appuyant sur leur expérience en matière de lutte contre les menaces susvisées, certains pays développés ont créé des systèmes nationaux de lutte contre la cybercriminalité pilotés par un organisme de coordination unique. Dans le même temps, les organismes gouvernementaux et non gouvernementaux concernés mettent en commun leurs forces et leurs ressources afin de combattre et de neutraliser les menaces contre la sécurité de l'information.

Il s'agit d'un aspect qui a occupé une place déterminante dans la révision des méthodes d'évaluation des risques et des défis nouveaux, en particulier dans le domaine de l'information, la mise en œuvre de mesures de haut niveau visant à créer un système national unique de lutte contre la cybercriminalité, l'élaboration d'un projet de loi ukrainien relatif à la cybersécurité et la mise en place et le renforcement de partenariats avec les services de renseignement et les organes chargés d'assurer le respect des lois d'autres pays.

En juin 2011, le Service de sécurité ukrainien, conjointement avec les services répressifs de 11 pays (États-Unis, Allemagne, Pays-Bas, Grande-Bretagne, Lettonie, Chypre, France, Lituanie, Roumanie, Canada et Suède), a mis fin aux activités d'un groupe international de pirates informatiques qui avait subtilisé plus de 72 millions de

dollars des États-Unis à des établissements bancaires étrangers en diffusant un logiciel malveillant sur Internet.

En octobre 2011, le Service de sécurité ukrainien a organisé et tenu à Yalta (Ukraine) des consultations d'experts annuelles Ukraine-OTAN sur la sécurité de l'information. Les participants ont soutenu la position de la partie ukrainienne, laquelle estimait nécessaire de continuer à renforcer la sécurité de l'information en faisant intervenir les secteurs public et privé et en s'appuyant sur l'expérience d'autres États.

À l'initiative du Service de sécurité ukrainien, il est prévu que les participants à la trente-deuxième session du Conseil des chefs de services de sécurité et de renseignement de la Communauté d'États indépendants réfléchissent à la création d'une commission chargée de la sécurité de l'information.

Les principes visés au paragraphe 2 (de la résolution 66/24 de l'Assemblée générale)

D'après la législation ukrainienne, entrent dans la catégorie des grandes menaces contre la sécurité nationale, notamment dans le domaine de l'information :

- Les actes limitant la liberté d'expression et l'accès à l'information;
- La criminalité et le terrorisme informatiques;
- La divulgation d'informations gouvernementales ou de tout autre type d'informations secrètes prévu par la loi, ainsi que d'informations confidentielles qui sont la propriété de l'État ou visent à répondre aux besoins et aux intérêts nationaux de la société et de l'État;
- Les tentatives de manipulation de l'opinion publique, en particulier par la diffusion d'informations fausses, incomplètes ou partisanes.

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

Pour garantir la sécurité de l'information à l'échelon international, il est essentiel de créer des conditions propres à assurer la sécurité de l'information de chaque État et d'instaurer une coopération efficace en la matière.

Si l'on veut lutter efficacement contre les risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information, il s'agit de prendre les mesures de coopération internationale suivantes :

- Créer des mécanismes consultatifs favorisant la coopération dans le domaine de la cybersécurité en vue d'échanger les expériences en ce qui concerne les lois et réglementations adoptées à ce sujet;
- Mettre en place un système d'échange de données de surveillance du cyberespace et un système d'alerte rapide en cas de cyberattaques, d'échange d'informations sur les aspects techniques des cyberattaques, d'identification de leur origine et de sélection de mesures de lutte efficaces;
- Coopérer en vue d'éliminer les conséquences négatives des cyberattaques, de faire la synthèse des expériences et de mettre au point des solutions techniques et des recommandations organisationnelles propres à prévenir les cyberattaques;

- Mettre au point des instruments juridiques internationaux destinés à établir une terminologie et des règles communes, comme un code de conduite sur Internet.

Compte tenu de la nécessité de lutter contre ces menaces, il semble indispensable de mettre en place des relations de coopération avec les organismes de renseignement et les services répressifs partenaires en vue de :

- Mettre en place des mécanismes permettant aux services de renseignement d'échanger rapidement les informations relatives aux actes commis par des groupes criminels organisés, notamment à caractère terroriste, et consistant à pirater les ressources informatiques de segments nationaux d'Internet et les systèmes d'information d'institutions gouvernementales et commerciales;
- Échanger des informations sur les infractions liées au piratage des systèmes informatiques d'institutions financières, lequel vise notamment à falsifier des cartes de paiement et à dérober des informations confidentielles ou perturber le fonctionnement de ces systèmes;
- Organiser la collaboration afin de retrouver les individus qui ont commis des infractions informatiques à l'aide des segments nationaux d'Internet et rassembler les preuves de leur activité illégale;
- Mettre en commun les expériences et les solutions disponibles en ce qui concerne l'examen des logiciels et du matériel informatique (ou les expertises judiciaires et cybernétiques) lors d'enquêtes relatives à des infractions commises à l'aide des technologies informatiques, et l'évaluation des méthodes d'investigation visant à rassembler des preuves de l'activité criminelle;
- Mettre en œuvre des programmes conjoints de formation professionnelle et organiser des stages à l'intention des experts des services de renseignement;
- Participer à des colloques, des conférences et des séminaires conjoints sur la lutte contre la cybercriminalité.

Dans le cadre de la coopération dans ce domaine, on pourrait notamment mettre en place des systèmes permettant de surveiller les ressources des segments nationaux d'Internet en vue de déceler les risques en temps utile et de trouver les moyens de les neutraliser au mieux.

Aux fins de la coordination des initiatives de prévention des atteintes à la sécurité informatique menées par les organismes gouvernementaux, les opérateurs de télécommunications et les autres acteurs de l'infrastructure nationale d'information, il pourrait être envisagé de créer des centres nationaux d'intervention en cas d'incident informatique, lesquels collaboreraient étroitement.

Ces centres nationaux seraient essentiellement chargés de :

- Collecter, analyser et stocker dans des bases de données des informations sur les risques actuels pesant sur la sécurité informatique;
- Surveiller et mettre en évidence les dispositifs et les ressources Internet dont le fonctionnement n'est pas conforme aux réglementations relatives aux activités des utilisateurs du segment national d'Internet;
- Élaborer, à l'intention des internautes, des recommandations visant à protéger les intérêts de la personne, de la société et de l'État en matière d'information et à leur proposer des services consultatifs et un appui technique;

- Recevoir des messages et fournir une assistance d'urgence permettant de mettre fin aux actes de piratage et d'avertir en temps voulu les internautes et les utilisateurs d'autres systèmes d'information, notamment les systèmes locaux et ceux des entreprises, des risques qui pèsent sur leur sécurité informatique;
- Coopérer et échanger des informations avec les centres analogues d'autres pays.