Nations Unies A/68/156

Assemblée générale

Distr. générale
16 juillet 2013
Français
Original : anglais/espagnol/russe

Soixante-huitième session
Point 94 de la liste préliminaire*
Progrès de l'informatique et des télécommunications et sécurité internationale

Progrès de l'informatique et des télécommunications et sécurité internationale

Rapport du Secrétaire général

Table des matières

* A/68/50.

13-39736 (F) 090813 120813

I. Introduction

1. Le 3 décembre 2012, l'Assemblée générale a adopté la résolution 67/27 intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale ». Au paragraphe 3 de sa résolution, l'Assemblée générale a invité tous les États Membres à continuer de communiquer au Secrétaire général, en tenant compte des constatations et recommandations figurant dans le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (A/65/201), leurs vues et observations sur les questions suivantes :

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

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

c) Les principes visés au paragraphe 2 de la résolution;

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

2. Pour donner suite à cette demande, une note verbale a été adressée aux États Membres le 22 février 2013 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]
[20 mai 2013]

L'utilisation malintentionnée des télécommunications ayant pour objectif déclaré ou non de porter atteinte à l'ordre juridique et politique des États constitue une violation des principes internationalement reconnus en la matière 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 67/27 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, Cuba condamne à nouveau la guerre audiovisuelle toujours plus agressive menée contre elle par le Gouvernement des États-Unis, 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.

Les émissions diffusées depuis des avions sont contraires au paragraphe 4 de l'article 42 du Règlement des radiocommunications de l'Union internationale des télécommunications (UIT) qui interdit aux stations d'aéronef en mer ou au-dessus de la mer d'effectuer un service de radiodiffusion.

En 2012, les États-Unis ont réalisé 192 vols, au moyen desquels ils ont non seulement émis illégalement des signaux de télévision en direction du territoire cubain, mais ils ont en même temps diffusé des émissions illégales dans la bande FM. Ces émissions ont créé un brouillage nuisible aux stations de télévision cubaines inscrites au Fichier de référence international des fréquences du Bureau des radiocommunications de l'UIT.

Chaque semaine, des émetteurs situés sur le territoire des États-Unis diffusent illégalement à Cuba 2 400 heures d'émissions radio et télévisées en moyenne via 30 différentes fréquences à ondes moyennes, courtes, FM et TV. Certains émetteurs, qui sont aux mains ou au service d'organisations liées à des éléments terroristes connus vivant sur le territoire des États-Unis, et y menant des activités anticubaines, diffusent des émissions incitant au sabotage, aux attentats politiques et au meurtre de personnalités et traitent d'autres sujets de prédilection du terrorisme des ondes.

La diffusion illégale d'émissions de radio et de télévision anticubaines entend inciter à l'immigration clandestine et à la violence, au non-respect de l'ordre constitutionnel et à la commission d'actes de terrorisme. Cuba rappelle qu'il est illégal d'avoir recours à l'information dans le but affiché de renverser l'ordre interne d'un autre État, de porter atteinte à sa souveraineté et de s'immiscer ou de s'ingérer dans ses affaires intérieures.

Ces émissions provocatrices hostiles à Cuba violent les dispositions internationales régissant l'utilisation du spectre radioélectrique de la Convention internationale des télécommunications, dont le Gouvernement américain est signataire.

Cuba a soutenu la résolution 67/27 de l'Assemblée générale et continuera de contribuer au progrès mondial de l'informatique et des télécommunications à des fins pacifiques, au profit de l'humanité tout entière.

Espagne

[Original : espagnol]
[29 mai 2013]

1. Introduction

La sécurité de l'information est un aspect essentiel de la société de l'information. Les progrès technologiques ont permis d'améliorer en continu et rapidement les capacités de traitement et de stockage de l'information sous de multiples formats. En outre, dans le domaine des communications, la largeur de bande disponible a nettement augmenté, ce qui permet de transmettre et de recevoir de très grandes quantités d'information, quasiment en temps réel et sans qu'il faille être doté d'infrastructures particulièrement complexes.

Mais, s'ils améliorent l'accès à toute sorte d'informations, ces progrès technologiques en facilitent également l'emploi ou l'accès à des fins illicites, à commencer par l'utilisation des systèmes de télécommunications et des systèmes informatiques à des fins hostiles ou criminelles, y compris aux fins de la commission d'actes de terrorisme ou d'agressions, entre États ou entre acteurs transnationaux.

Ces dernières années, la tendance s'est confirmée : les organisations criminelles, et en particulier les groupes terroristes, ont de plus en plus recours à Internet, exploitant essentiellement deux de ses caractéristiques, à savoir son universalité et l'anonymat qu'il peut offrir.

Il est donc nécessaire de concilier l'évolution de la société et des technologies de l'information et celle, parallèle, de normes nationales et internationales, actualisées, modernes, adaptées au nouveau contexte technologique et aptes à répondre aux problèmes que pose la nécessité de protéger l'information pour en empêcher l'usage illicite sans pour autant limiter les droits ni les libertés de la personne.

2. Utilisation d'Internet à des fins terroristes

Actuellement, les principales menaces que fait peser l'emploi d'Internet par des organisations terroristes sont les suivantes :

a) Usage offensif comme moyen d'attaquer les systèmes informatiques d'infrastructures critiques ou l'infrastructure même d'Internet. Ces attaques sont relativement fréquentes et relèvent de la délinquance ordinaire mais celle qu'a subie l'Estonie en 2007 a montré que l'infostructure d'un État peut s'effondrer lorsqu'elle est victime de ce type d'attaque. Dans cet ordre d'idées, les logiciels malveillants apparus ces dernières années et les « botnets », ou réseaux d'ordinateurs « zombies » qui servent à attaquer les systèmes informatiques se multiplient.

b) Usage servant à d'autres activités, essentiellement les suivantes :

- **Activités de communication**. Le Web supplante les moyens de communication classiques utilisés par les organisations criminelles, comme la téléphonie fixe ou la téléphonie mobile. Les moyens de communication par Internet les plus utilisés sont le courrier électronique, les programmes de messagerie instantanée et les forums;
- **Diffusion de propagande et de documentation liées à des activités terroristes**. Il existe actuellement des milliers de sites Web liés à des activités terroristes ou qui incitent à la violence, tendance qui s'est amplifiée avec l'apparition du phénomène Web 2.0 et des réseaux sociaux. Or, il est très difficile d'empêcher les organisations terroristes de se servir ainsi du Web car ces sites migrent très facilement. Il s'agit d'un phénomène transnational car le serveur hôte peut se trouver dans un pays différent de celui à partir duquel la page est administrée et de celui où opère l'organisation terroriste en question, ce qui crée un vide juridique si les pays concernés n'ont pas conclu d'accords bilatéraux;
- **Activités de recrutement**. Il arrive qu'Internet, surtout les forums et les programmes de messagerie instantanée, serve à enrôler de nouvelles recrues;

- **Financement. Internet permet aux organisations terroristes de mener des activités de collecte de fonds**. La possibilité de participer à la commission de fraudes ou d'actes d'extorsion ou encore au blanchiment d'argent comme moyen de lever des fonds est particulièrement attrayante pour les organisations;
- **Diffusion de manuels d'entraînement**. Par Internet, les organisations terroristes diffusent des manuels sur les techniques du terrorisme, la fabrication d'explosifs ou le maniement d'armes;
- **Mine d'informations pour commettre des attentats**. Internet constitue une source d'information très riche que les organisations terroristes utilisent dans bien des cas pour se renseigner sur leur cible, qu'il s'agisse de personnes, d'organisations ou d'infrastructures.

3. Mesures prises à l'échelle nationale pour lutter contre l'utilisation d'Internet par les organisations terroristes

3.1. Mesures législatives

Au cours des dernières années, et particulièrement en 2007, l'Espagne a déployé d'importants efforts pour se doter de mesures en la matière en introduisant dans son ordre juridique une série de lois visant la sécurité de l'information et le libre exercice des droits et libertés reconnus dans la Déclaration universelle des droits de l'homme et dans la Constitution. Une législation et une réglementation exhaustives, comprenant aussi bien des textes portant sur des questions purement nationales que des dispositions incorporant des directives de l'Union européenne, ont été élaborées en fonction de nouveaux critères de sécurité de l'information, selon lesquels, pour que la protection soit suffisante, il faut non seulement préserver la confidentialité des informations mais aussi et surtout veiller autant que possible à en préserver l'intégrité et la disponibilité. À signaler notamment :

- La loi organique 5/1992 du 29 octobre 1992 sur le traitement automatisé des données personnelles, et ses mesures d'application, visant à instaurer des mécanismes permettant d'éviter les atteintes à la vie privée résultant du traitement de l'information;
- La loi organique 15/1999 du 13 décembre 1999 sur la protection des données personnelles et ses mesures d'application, visant à garantir et protéger les libertés publiques et les droits fondamentaux des personnes physiques, et notamment leur honneur et leur vie privée et familiale;
- Le décret-loi royal 14/1999 du 17 septembre 1999 sur la signature électronique, adopté afin de favoriser rapidement l'usage des nouvelles technologies de sécurité des communications électroniques par les entreprises, les citoyens et les administrations publiques, qui a transposé dans l'ordre juridique espagnol la directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques. La loi 59/2003 du 19 décembre 2003 sur la signature électronique modifie ce cadre pour tenir compte de l'expérience acquise depuis son entrée en vigueur;

- La loi 11/2002 du 6 mai 2002 relative au Centre national du renseignement (CNI) puis le décret royal 421/2004 du 12 mars 2004 relatif au Centre national de cryptologie, par lesquels le CNI est notamment chargé de coordonner l'action des différents services publics qui utilisent des méthodes et procédures de chiffrage, de garantir la sécurité informatique et de veiller au respect des normes relatives à la protection de l'information classifiée;
- La loi 34/2002 du 11 juillet 2002 sur les services de la société de l'information et du commerce électronique. Elle a pour objet de transposer dans l'ordre juridique espagnol la directive 2000/31/CE, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur (« directive sur le commerce électronique »). De même, elle transpose partiellement la directive 98/27/CE du Parlement européen et du Conseil, du 19 mai 1998, relative aux actions en cessation en matière de protection des intérêts des consommateurs, et régit, conformément aux dispositions de la directive, l'action en cessation contre les conduites qui contreviennent à cette loi;
- La loi 32/2003 du 3 novembre 2003 sur les télécommunications, qui régit l'exploitation des réseaux et la prestation des services de communication électronique;
- La loi 59/2003 du 19 décembre 2003 sur la signature électronique, susmentionnée;
- La loi 11/2007 du 22 juin 2007 sur l'accès électronique des citoyens aux services publics, qui régit les communications par voie électronique, informatique et télématique entre les citoyens et les administrations publiques;
- La loi organique 10/2007 du 8 octobre 2007 relative à la base de données policières pour l'identification à partir de l'acide désoxyribonucléique (ADN), portant création d'une base de données regroupant pour la première fois les fichiers des forces et des organes de sécurité de l'État dans lesquels sont stockées les données d'identification obtenues à partir d'analyses d'ADN effectuées dans le cadre d'enquêtes criminelles ou lors de l'identification de cadavres ou la recherche de personnes disparues;
- La loi 25/2007 du 18 octobre 2007 sur la conservation des données relatives aux communications par voie électronique et aux réseaux publics de communications, qui facilite la conduite des enquêtes dans ce domaine;
- Le décret royal 1720/2007 du 21 décembre 2007, approuvant le règlement d'application de la loi organique 15/1999 du 13 décembre 1999 sur la protection des données personnelles;
- La loi 56/2007 du 28 décembre 2007 sur les mesures d'incitation visant à établir la société de l'information;
- Les infractions cybernétiques liées aux activités d'organisations terroristes sur Internet énumérées ci-après ont été inscrites dans le code pénal :
  - Sabotages informatiques (art. 264);
  - Menaces (art. 169 et suiv.);
  - Apologie et éloge du terrorisme (art. 578).

3.2. Autres mesures

- Création de groupes de police chargés de lutter contre l'utilisation d'Internet par les groupes criminels
- Participation au projet « Check the Web » de l'Office européen de police (Europol)
- Le Centre national de cryptologie du Centre national du renseignement (CNI) contribue quotidiennement et de manière décisive à la lutte contre les attaques cybernétiques, essentiellement grâce à l'activité du CCN-CERT (équipe d'intervention informatique d'urgence) qui est doté des moyens de faire face aux problèmes de sécurité de l'information. Créée début 2007 au service du Gouvernement espagnol, cette équipe est présente dans les principales instances internationales où sont examinés les objectifs, les idées et les informations relatifs à la cybersécurité
- Création du Centre national de protection des infrastructures critiques
- Le Ministère de la défense a lancé plusieurs initiatives dans le domaine de la cyberdéfense. Ainsi, l'état-major des armées participe au Centre d'excellence pour la cyberdéfense de l'Organisation du Traité de l'Atlantique Nord (OTAN) à Tallín) que l'Espagne cofinance depuis sa création et auquel elle fournit deux experts. Ce centre joue un rôle de plus en plus important sur le plan international dans la lutte contre le cyberterrorisme, comme en témoigne la récente visite de S. M. le Roi d'Espagne qui a mis l'accent sur la participation de l'Espagne à l'action internationale en faveur de la cybersécurité
- Par ailleurs, l'OTAN s'emploie activement à mettre en place des activités de cyberdéfense et a notamment élaboré un concept, formulé une politique et créé un Bureau de gestion de la cyberdéfense
- L'Organisation pour la sécurité et la coopération en Europe (OSCE) a établi un groupe de travail informel chargé de mettre en place des mesures de confiance visant à réduire les risques de conflit découlant de l'utilisation des technologies de l'information et des communications. Ce groupe de travail cherche à réduire les risques de cyberattaques et, parallèlement, à renforcer la sécurité entre États en favorisant la coopération internationale, la clarté et la transparence et en évitant les malentendus qui pourraient conduire à une escalade des conflits, le tout grâce à des mesures de renforcement de la confiance aux niveaux politique et militaire dans le domaine de l'utilisation des technologies de l'information et de la communication
- Plan national de sécurité. Il fixe la politique de sécurité nationale qui régit l'utilisation des médias électroniques. Fondé sur des principes fondamentaux et des conditions minimales qui assurent une protection adéquate de l'information, il concerne toutes les administrations. Un décret royal qui lui servira de fondement juridique sera publié prochainement, en application de l'article 42 de la loi 11/2007. De fait, la stratégie nationale de sécurité, qui précise les menaces et les risques les plus graves qui pèsent sur la sécurité du pays et les moyens d'y faire face, cite le cyberespace comme l'un des domaines dans lesquels il convient d'agir. Cette analyse sert de point de départ pour la formulation de lignes stratégiques, le renforcement des capacités et l'élaboration des réformes structurelles

La directive de 2012 relative à la défense nationale, qui énumère les menaces mondiales à enrayer, place les cyberattaques au premier rang des risques et précise qu'elles ne pourront être jugulées qu'à l'aide d'une coalition de forces (dans le cas de l'Espagne, l'OTAN et l'Union européenne) et qu'il faudra en outre obtenir l'appui d'autres pays ou groupes de pays directement et également concernés par la maîtrise de ces phénomènes.

De même, cette directive a comme fil directeur la mise en place d'une gestion intégrée de la cybersécurité dans le cadre des principes établis à cet effet dans la stratégie nationale de cybersécurité.

Elle qualifie le cyberespace de nouveau volet des relations internationales et considère qu'il faut absolument renforcer les moyens d'obtention de l'information et les mécanismes de renseignement sur lesquels s'appuient les opérations, ainsi que les dispositifs de commandement et de contrôle, afin de réduire les risques d'attaques cybernétiques.

En janvier 2011, le chef d'état-major de la défense a publié un document exposant son point de vue sur la cyberdéfense militaire, qui vise à préciser la définition et à guider le déploiement et l'utilisation des ressources militaires nécessaires pour rationaliser l'usage du cyberespace dans les activités militaires.

4. Mesures que pourrait adopter la communauté internationale pour renforcer la sécurité informatique à l'échelle mondiale

La sécurité du cyberespace est devenue un facteur essentiel pour la bonne marche de l'État moderne, de plus en plus tributaire des systèmes informatiques et de l'interconnexion des infrastructures critiques. Elle doit donc faire partie intégrante de la planification de la sécurité nationale.

À l'heure actuelle, aucun cadre juridique international ne permet de faire face aux menaces qui pèsent sur la cybersécurité, de sorte que, sans pour autant renoncer à la souveraineté nationale, il serait bon de conclure des accords multilatéraux de collaboration en la matière (analogues à la Convention internationale pour la sauvegarde de la vie humaine en mer) par lesquels les États s'engageraient à harmoniser leur législation pour permettre la poursuite des cyberinfractions, afin d'éviter, dans la mesure du possible, que l'anonymat, l'absence de législation et les intérêts économiques fassent du Web le terrain idéal pour la délinquance et le terrorisme.

Il faut que le secteur privé, en particulier les fournisseurs d'accès à Internet, participe à la lutte contre la cyberdélinquance. Son concours est essentiel car la majorité des services Internet est entre ses mains. Il consacre beaucoup de temps à faire face aux menaces sur Internet et ses connaissances et son expérience peuvent être très utiles.

Les équipes d'intervention informatique d'urgence sont la clef de voûte de la cybersécurité. L'établissement de telles équipes spécialisées et la formation continue de leurs membres, ciblée sur la connaissance des dernières tendances, sont les premières mesures que les États doivent prendre pour garantir la cybersécurité. Il est aussi important de créer au sein des forces chargées du maintien de l'ordre des unités spécialisées chargées d'enquêter sur les infractions commises au moyen d'Internet.

La cybersécurité représente un défi mondial et il est donc fondamental pour l'améliorer de promouvoir la coopération internationale aux niveaux politique et opérationnel. Les échanges entre les équipes d'intervention informatique d'urgence des différents pays doivent êtres très fluides de manière à faciliter le partage des informations sur les attaques, avec un temps de réaction minimal. Les leçons tirées de l'expérience et les pratiques optimales doivent aussi être mises en commun.

Autres mesures proposées :

- Formation et sensibilisation des citoyens depuis leur plus jeune âge afin qu'ils demeurent attentifs à la sécurité des systèmes informatiques qu'ils utilisent. De nombreuses formes de cybercriminalité profitent (voire dépendent) du fait que les utilisateurs d'Internet ne prennent pas toutes les précautions voulues pour rendre leurs ordinateurs et leurs comptes aussi sûrs et inaccessibles que possible. Il est donc essentiel de bien former les utilisateurs. Une plus grande prise de conscience de ce problème permettrait de réduire le nombre des ordinateurs utilisés par les cyberdélinquants pour mener leurs activités, en particulier celles qui sont liées aux « botnets »;

- Assouplissement des procédures de coopération internationale en matière judiciaire et policière afin que les auteurs d'infractions pénales puissent être poursuivis rapidement et efficacement selon la législation de chaque pays, la structure d'Internet étant fragmentée et les registres éphémères;

- Organisation de colloques, de conférences et de séminaires internationaux visant à perfectionner les connaissances des experts et à partager les informations relatives aux différentes formes d'attaques, aux nouvelles tendances, à l'analyse des risques et aux effets d'éventuelles attaques. Il s'agirait également de mettre en commun les leçons tirées de l'expérience et les pratiques optimales et de promouvoir l'harmonisation de la formation dispensée aux membres des forces de l'ordre chargés d'enquêter sur la cyberdélinquance;

- Coordination des initiatives avec d'autres organisations spécialisées dans certains aspects de la cybercriminalité, comme le Conseil de l'Europe et l'OTAN. Cela permettrait d'éviter les doubles emplois;

- Élaboration de guides et d'inventaires des bonnes pratiques en vue d'améliorer la cybersécurité, en coopération avec le secteur privé et la société civile.

En conclusion, la communauté internationale devrait prendre les mesures de protection de l'information qui s'imposent, en se fondant sur une stratégie homogène et, si possible, en imprimant une orientation unique en vue d'établir des normes et des critères applicables à tous les pays et de mettre en place un ensemble cohérent et complet de mesures de protection concrètes permettant d'harmoniser les politiques et l'action des différentes organisations nationales et internationales concernées.

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

[Original : anglais]
[16 mai 2013]

Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord se félicite de l'occasion qui lui est donnée de répondre à la résolution 67/27 de l'Assemblée générale intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale ».

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

Dans le présent exposé, le Royaume-Uni privilégie le terme « cybersécurité » et les expressions connexes lorsqu'il se réfère aux mesures visant à préserver la confidentialité, la disponibilité et l'intégrité des informations du cyberespace. Le terme « sécurité de l'information », souvent utilisé par les organisations professionnelles et les organismes de normalisation, a la même signification. Le Royaume-Uni accepte également cette formulation, qui peut cependant prêter à confusion dans la mesure où certains pays et certaines organisations l'utilisent à propos d'une doctrine selon laquelle l'information constitue une menace contre laquelle il convient de prévoir une protection supplémentaire. Le Royaume-Uni ne reconnaît pas cet emploi particulier de l'expression « sécurité de l'information », qui est susceptible d'être utilisée pour légitimer des restrictions de la liberté d'expression portant atteinte aux principes de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques.

Domaine très prometteur, le cyberespace représente néanmoins une menace réelle et potentielle. Plus de 2 milliards de personnes s'y côtoient désormais par l'entremise du réseau Internet et ce nombre devrait encore progresser puisque les technologies mobiles permettent aux pays en développement de tirer parti de ses immenses avantages à moindre coût. Le réseau Internet représente un moteur pour la croissance économique, ouvre la voie à l'éducation, amène les êtres humains à échanger davantage et à mieux se comprendre, brise les barrières culturelles et géographiques, permet la prestation de services à distance et renforce la démocratie en rendant les autorités comptables de leurs actes vis-à-vis des populations, selon des modalités nouvelles et dynamiques. À titre d'exemple :

- Les activités reposant sur Internet contribuent déjà à hauteur de 8 % au PIB du Royaume-Uni. Il est capital, pour la croissance économique, que le cyberespace inspire suffisamment confiance aux entreprises et à leurs clients pour leurs activités;
- Le Royaume-Uni a mis en place en 2011 un service de pétitions en ligne, qui permet à quiconque de lancer ou de signer une pétition relative à un problème impliquant les autorités. Toutes les pétitions réunissant au moins 100 000 signatures font l'objet d'un débat devant le Parlement. Au cours de la première année de fonctionnement de ce service, plus de 15 600 pétitions ont été ainsi lancées. Dix d'entre elles, qui ont dépassé le seuil des 100 000 signatures, ont fait ou doivent faire l'objet d'un tel débat.

À l'instar de nombreux pays, le Royaume-Uni dépend du cyberespace pour de nombreux services primordiaux tels que l'énergie, la finance et les transports. Toute

défaillance importante concernant ces services, qu'elle soit accidentelle ou due à une intrusion délibérée, pourrait occasionner de graves perturbations, des dommages économiques, ou la perte de vies humaines.

L'horizon des menaces est aussi complexe que mouvant. Les systèmes de l'État britannique sont chaque jour l'objet, tout comme ceux des entreprises et des particuliers, de tentatives d'intrusion ayant des motivations aussi diverses que l'espionnage politique et industriel, la cybercriminalité, la volonté de perturber les réseaux ou d'en prendre le contrôle, ou le déni de service. Ces menaces peuvent émaner d'États ou de leurs agents, d'acteurs non étatiques, d'organisations criminelles ou d'individus opportunistes. En raison du caractère interconnecté du cyberespace, toute activité affectant un système peut atteindre de façon inattendue et imprévisible d'autres systèmes. La lutte contre ces menaces se heurte à la difficulté de déterminer avec certitude la source d'un cyberincident, à la possibilité qu'ont les coupables de se faire passer pour d'autres, à la méconnaissance, de la part de certains États, des règles de bonne conduite dans le cyberespace, au manque de résilience de l'infrastructure des réseaux de certains pays et à l'absence d'harmonisation, au niveau international, pour ce qui est de l'identification des cybercriminels, ainsi que des poursuites et des procédures menées à leur encontre.

Toutes les composantes de la société ont un rôle à jouer et des responsabilités à assumer dans la lutte contre ces menaces. C'est aux gouvernements qu'il appartient de conduire les efforts faits au niveau international pour parvenir à mieux s'entendre sur les comportements acceptables de la part de l'État et de régler le problème de la cybercriminalité, mais comme les infrastructures sont majoritairement détenues et exploitées par des entreprises privées, il est essentiel que ces dernières participent au débat. Le Royaume-Uni estime que l'amélioration de la cybersécurité ne doit pas porter préjudice aux avancées économiques et sociales dont le cyberespace est porteur. Il est particulièrement important de faire en sorte que les efforts déployés pour accroître la cybersécurité ne soient pas détournés pour imposer des restrictions à la liberté d'expression outrepassant celles qu'autorisent les accords internationaux. À cet égard, le rôle des organisations de la société civile est particulièrement important.

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

Stratégies nationales

Les cyberattaques constituent, avec les crises militaires internationales, les accidents graves ou les catastrophes naturelles et les attaques terroristes, l'une des quatre menaces de première catégorie répertoriées dans la stratégie de sécurité nationale que le Royaume-Uni a rendue publique en 2010. En novembre 2011, le Royaume-Uni a présenté une mise à jour de cette stratégie, qui envisage un cyberespace dynamique, résilient et sécurisé, porteur de bienfaits économiques et sociaux considérables, où ces valeurs fondamentales que constituent la liberté, l'équité, la transparence et la primauté du droit contribuent à renforcer la prospérité, la sécurité nationale et la cohésion de la société. Cette stratégie prévoit quatre objectifs :

- Lutter contre la cybercriminalité et être l'un des endroits les plus sûrs au monde pour exercer une activité économique dans le cyberespace;

- Mieux résister aux cyberattaques et être capables de mieux protéger nos intérêts dans le cyberespace;
- Contribuer à façonner un cyberespace ouvert, stable et dynamique que le public britannique puisse utiliser en toute sécurité et qui soutienne les sociétés ouvertes;
- Disposer des connaissances, des compétences et des capacités transversales dont nous avons besoin à l'appui de nos ambitions en matière de cybersécurité.

Pour que ces objectifs puissent être atteints, le Gouvernement britannique a alloué 650 millions de livres sterling de dépenses supplémentaires à un programme quadriennal visant à modifier les dispositions prises pour faire face aux cybermenaces.

Le Royaume-Uni a investi dans un dispositif nouveau et sans équivalent afin de protéger ses réseaux et ses services de base et d'approfondir sa compréhension de la menace à laquelle il doit faire face. Cette compréhension lui permet de mieux hiérarchiser et de mieux orienter ses mesures de protection. Sous les auspices du Ministère de la défense, il a mis en place une entité comportant trois composantes, chargées de mettre au point des tactiques, des techniques et des stratégies nouvelles visant à mettre sur pied une capacité de riposte militaire à des menaces sophistiquées. Le Gouvernement collabore étroitement avec les victimes de la cyberactivité et utilise les enseignements de cette concertation pour conseiller les entreprises afin qu'elles améliorent leurs mesures de cybersécurité. En ce qui concerne ses propres réseaux, il est en train de mettre au point un nouveau modèle pour sécuriser l'échange de services, avec notamment des protocoles d'authentification du personnel plus élaborés, un meilleur contrôle de la conformité et une plus grande résilience du réseau.

Le Gouvernement britannique a investi dans le renforcement des capacités de la police et de la justice à prévenir la cybercriminalité, à y mettre un terme, à mener des enquêtes et à traduire les responsables en justice. La Police Contral e-Crime Unit (Service central de lutte contre la cybercriminalité de la police) a triplé de volume, trois équipes régionales de cyberpoliciers ont été constituées et une formation sur la lutte contre la cybercriminalité a été conçue à l'intention des policiers généralistes. La Serious Organized Crime Agency (Agence de lutte contre la grande criminalité organisée) va fusionner avec le Service central de lutte contre la cybercriminalité en 2013 pour former une nouvelle entité dénommée « National Cybercrime Unit of the National Crime Agency », ce qui représente une nouvelle étape vers l'amélioration des capacités de répression de la cybercriminalité au Royaume-Uni.

L'industrie britannique est la principale victime d'une cybercriminalité dont le vol de propriété intellectuelle à grande échelle constitue l'un des aspects. Le Gouvernement, qui s'efforce avec l'industrie et les universités de faire savoir qu'il est nécessaire de lutter contre les cybermenaces, a publié en 2012 un document d'orientation à l'intention des chefs d'entreprise, montrant comment les cadres supérieurs devraient adopter des stratégies visant à protéger leurs informations les plus sensibles. Il a également mené à bien une initiative de partage d'information pilote en vue de créer un environnement fiable pour l'échange, entre organisations, de données sur les menaces actuelles et sur la gestion des problèmes. Cette initiative

réunit environ 160 entreprises des secteurs de la défense, des finances, de l'industrie pharmaceutique, de l'énergie et des télécommunications.

En collaboration avec l'industrie, le Gouvernement britannique s'est employé à mettre en garde les professionnels et le public contre les menaces qui planaient, de façon à les inciter à adopter les mesures, souvent simples, à même de les protéger et à exiger que les produits et les services informatiques soient plus sûrs. Les initiatives suivantes s'inscrivaient dans le cadre de cette action : la semaine « Get Safe Online » (organisée avec l'Union européenne et le Canada), des campagnes ciblées sur la fraude en ligne menées par la National Fraud Authority (Autorité nationale de répression des fraudes), et une campagne intitulée « Devils in your details », organisée en 2012.

Le Royaume-Uni investit dans les compétences et dans la recherche afin de se doter de moyens propres à lui permettre de continuer de faire face à ces problèmes. Les huit premières universités britanniques qui se sont lancées dans la recherche sur la cybersécurité se sont vues dotées du statut de « Centre d'excellence universitaire sur la recherche en cybersécurité ». En ce qui concerne le système éducatif, des supports pédagogiques interactifs à l'usage des enfants d'âge scolaire sont en cours d'élaboration et un programme d'apprentissage technique, dont le but est de repérer les élèves plus âgés et les étudiants doués et d'améliorer leurs compétences, a été lancé. Le référentiel de compétences des professions de l'information sécurisée permettra de vérifier les compétences et la formation des professionnels de la cybersécurité, ce qui aidera le secteur privé et le secteur public à recruter les bonnes personnes au bon niveau et au bon poste.

Stratégies internationales

Le Royaume-Uni est à la pointe de l'action internationale en faveur de l'amélioration de la transparence, de la prévisibilité et de la stabilité du cyberespace. En novembre 2011, le pays a accueilli la première Conférence internationale sur le cyberespace, qui a permis aux représentants de plus de 60 pays, d'entreprises et d'organisations de la société civile, de débattre sur les moyens d'étendre les avantages que procure le cyberespace sur les plans économique et social, de la coopération dans la lutte contre la cybercriminalité, de la sécurité et de la fiabilité de l'accès à Internet et de la sécurité internationale. Le mouvement enclenché lors de cette manifestation a été relancé en 2012 lors de la conférence qui s'est tenue à Budapest et une autre conférence, qui devrait avoir lieu à Séoul en 2013, est déjà en préparation.

Le Royaume-Uni est membre du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, ainsi que du Groupe de travail informel de l'Organisation pour la sécurité et la coopération en Europe relatif à l'instauration de mesures de confiance pour le cyberespace.

En octobre 2012, le Royaume-Uni a annoncé la création d'un centre pour le renforcement des capacités en matière de cybersécurité mondiale, doté d'un financement de 2 millions de livres sterling par an, consacré à diverses initiatives multilatérales et bilatérales. Ce centre proposera à d'autres pays, de façon indépendante, des conseils et des services spécialisés concernant la mise en place d'infrastructures nationales plus sûres et plus résilientes, et deviendra une plaque

tournante pour la recherche de haut niveau et la collaboration internationale sur cette question essentielle.

Avec l'objectif de participer à la lutte internationale contre la cybercriminalité mondiale, le Royaume-Uni continue de promouvoir la Convention sur la cybercriminalité, qu'elle considère comme l'instrument le plus efficace dans ce domaine, et ses principes. L'Agence de lutte contre la grande criminalité organisée continue, avec ses partenaires internationaux, à jouer un rôle mondial de premier plan pour ce qui est de porter les problèmes de répression des infractions à l'attention de l'ICANN, organisation chargée d'administrer les noms de domaines d'Internet.

Principes internationaux devant permettre de renforcer la sécurité des systèmes informatiques et télématiques mondiaux

Le concept clef est l'application du droit international et des normes régissant le comportement des États entre eux. Le Royaume-Uni est fermement convaincu que ces principes s'appliquent également au cyberespace et que, si les États affirment sans équivoque que les activités qu'ils mènent dans cet univers doivent être régies par ces lois et ces normes, ils jetteront les bases d'un cyberespace plus pacifique, plus prévisible et plus sûr.

À cet égard, le cyberespace pose des problèmes particuliers, tels que la difficulté de déterminer avec certitude l'origine d'une activité donnée, l'évaluation de l'intention et le rôle des acteurs non étatiques. Le Royaume-Uni appelle de ses vœux un débat au niveau mondial sur les modalités d'application du droit international et des normes relatives au comportement des États dans cet environnement.

Le Royaume-Uni ne croit pas que les efforts faits pour élaborer des traités multilatéraux, des codes de conduite ou des instruments similaires d'une portée globale puissent contribuer à améliorer la cybersécurité dans un avenir prévisible. Tout accord contraignant portant sur la totalité d'un cyberespace qui évolue « à la vitesse du Net » serait par définition complexe et exhaustif. Un tel instrument ne pourrait ni être efficace, ni emporter une large adhésion, sans que soit mené pendant de nombreuses années, voire des décennies, un travail laborieux sur les normes de conduite et les mesures de confiance qui s'imposent pour que s'établisse un nécessaire climat de compréhension et de confiance entre les signataires, et pour que ces derniers puissent être réellement tenus pour responsables de la tenue de leurs engagements. L'expérience acquise, dans d'autres domaines, lors de la conclusion de ce type d'accords, montre qu'ils ne peuvent être utiles et efficaces que s'ils constituent l'aboutissement, et non le point de départ, d'activités diplomatiques visant à obtenir une communauté de vues et une approche commune. Le Royaume-Uni estime que la communauté internationale devrait axer ses efforts sur l'obtention d'une position commune au sujet des normes et du droit internationaux, au lieu de négocier des instruments contraignants qui ne feraient que conduire à l'imposition partielle et prématurée d'une certaine doctrine à un domaine qui pour l'instant n'a pas la maturité requise.

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

Le cyberespace étant par définition transfrontalier, les États se doivent de renforcer la coopération bilatérale, régionale et multilatérale pour élaborer des mesures communes face à des menaces qui sont communes. De l'avis du Royaume-Uni, les mesures les plus utiles seraient les suivantes :

a) Poursuite des discussions entre États en vue d'élaborer un cadre normatif déterminant les comportements acceptables de la part des États, fondé sur les principes du droit international et sur les normes du droit coutumier international en vigueur;

b) Mise au point, pour le cyberespace, de mesures de confiance visant à rendre le comportement des États plus transparent et plus prévisible, et donc à réduire le risque d'une mauvaise interprétation ou d'une multiplication involontaire des incidents;

c) Mise en place, par les États, d'équipes d'intervention informatique d'urgence jouant le rôle de plaque tournante dans la gestion des incidents et le partage de l'information, complétée par la notification des principaux points de contact et par des mécanismes de communication en situation de crise fiables;

d) Mise au point d'exercices conjoints pour tester la gestion collective des incidents et les procédures de communication;

e) Élaboration de cadres juridiques harmonisés pour lutter contre la cybercriminalité;

f) Renforcement du dialogue avec les représentants des entreprises et de la société civile pour garantir la coordination et la hiérarchisation des approches dans un domaine en grande partie détenu et exploité par le secteur privé;

g) Aide au renforcement des capacités en matière de cybersécurité prodiguée par les États dotés des moyens les plus élaborés aux autres États.

Ukraine

[Original : russe]
[31 mai 2013]

1. Vue d'ensemble des problèmes relatifs à la sécurité informatique

Dans sa politique nationale de sécurité, l'Ukraine accorde une place essentielle à la sécurité informatique, de même qu'à celle des télécommunications et à la lutte contre la cybercriminalité, et elle œuvre de ce fait au renforcement de la sécurité internationale dans le contexte de la mondialisation.

La mondialisation, l'émergence d'une société de l'information et l'introduction de nouvelles technologies rendent encore plus nécessaire l'établissement d'une politique nationale de sécurité incluant un volet informatique, qui permette de protéger les intérêts nationaux dans ce domaine des menaces tant intérieures qu'extérieures.

Les menaces pesant sur la sécurité informatique à l'échelle internationale sont les suivantes :

- Utilisation illégale des ressources informatiques;
- Actions non autorisées à caractère destructeur visant les systèmes informatisés, notamment ceux qui régissent les sites des infrastructures nationales clefs;
- Utilisation du cyberespace, ainsi que de réalisations, techniques et moyens informatiques, d'une manière attentatoire aux droits fondamentaux et aux libertés individuelles, ou en vue de l'accomplissement d'actes terroristes ou extrémistes ou d'autres actes criminels pouvant aller jusqu'à l'agression;
- Utilisation de l'outil informatique en vue de diffuser des informations à caractère hostile ou haineux dans la société ou dans un pays donné;
- Diffusion d'informations contrevenant à la législation en vigueur, ainsi qu'aux règles et principes de la morale;
- Utilisation du cyberespace aux fins de la déstabilisation de la société, de l'attaque des fondements économiques, politiques et sociaux d'un État tiers, ou de la désinformation visant à porter atteinte à des valeurs culturelles, morales et esthétiques;
- Entrave à l'accès aux nouvelles technologies et création de conditions favorisant la dépendance technologique en matière d'informatisation, afin d'en retirer des bénéfices et d'être en mesure de contrôler le cyberespace d'États tiers.

D'autres problèmes découlant de la mondialisation méritent une attention particulière, dans le domaine de l'information; il s'agit de l'influence qu'exerce l'informatique sur la conscience individuelle et collective, des restrictions d'accès aux services informatiques et de la cybercriminalité.

Les spécialistes ukrainiens du domaine ont estimé que la probabilité de voir se concrétiser les menaces susmentionnées augmentait en fonction des facteurs suivants :

- Faible niveau des connaissances informatiques chez la majorité des utilisateurs de ressources et de services informatiques;
- Absence d'un cadre conceptuel unique en matière de sécurité informatique, à l'échelle internationale;
- Divergence d'approche des législations nationales en ce qui concerne les mesures de protection de l'information visant à créer et à moderniser (remettre en état) les infrastructures informatiques;
- Hétérogénéité des niveaux d'informatisation et de sécurité de l'information d'un pays à l'autre;
- Danger potentiel inhérent à la connexion de systèmes télématiques et de dispositifs pouvant s'avérer destructeurs;
- Absence de directives précises permettant d'identifier l'origine des opérations non autorisées effectuées dans le cyberespace.

2. Efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine

En Ukraine, les principaux organes publics chargés de la sécurité informatique et de ses composantes sont le Ministère des affaires intérieures, le Service de sécurité et le Service public chargé des communications spéciales et de la protection de l'information. Ces organismes interviennent activement dans la réglementation des différents aspects relatifs à la sécurité de l'information, en accordant une attention particulière au cadre juridique et réglementaire de sa composante cybernétique (cybersécurité).

En Ukraine, les relations sociales relevant du domaine de la sécurité informatique sont régies par les normes juridiques indiquées ci-dessous.

En vertu de l'article 17 de la Constitution ukrainienne, l'État porte la responsabilité principale de la sécurité informatique au même titre qu'il est le garant de la souveraineté et de l'intégrité territoriale, et qu'il assure le bon fonctionnement de l'économie.

En vertu de l'article 3 de la loi sur l'information, la sécurité informatique relève des principales orientations fixées par l'État dans la politique qu'il conduit en matière d'information.

La sécurité informatique occupe une place particulière au sein de l'appareil de sécurité ukrainien dans la mesure où les échanges et procédures informatiques sont au cœur de la vie sociale et étatique. Par ailleurs, on considère qu'elle est déterminée par l'état de l'espace informatique (environnement), composé de l'ensemble des infrastructures, technologies, ressources et échanges entre les intervenants, par lequel il est fait en sorte que le développement et l'utilisation des moyens informatiques servent l'intérêt des personnes, de la société et de l'État.

Les principaux objectifs de la sécurité informatique découlent des priorités fixées en matière de sécurité nationale et répondent aux exigences du développement social. Ils se définissent comme suit :

- Garantir la souveraineté nationale en matière d'informatique dans le contexte de la mondialisation des processus y relatifs et des visées dominatrices des autres pays dans ce domaine;
- Créer un environnement informatique axé sur le développement des valeurs spirituelles et des ressources intellectuelles des personnes et de la société dans son ensemble;
- Aider au maintien du volume adéquat de ressources informatiques permettant le fonctionnement permanent de la société et de l'État et le développement personnel;
- Protéger les informations relatives aux personnes physiques et juridiques et à l'État des menaces informatiques tant extérieures qu'intérieures, en luttant entre autres contre les délits informatiques;
- Assurer le respect de la légalité et l'exercice des droits des intervenants ukrainiens dans les domaines de la création et de l'utilisation des ressources, des techniques et des infrastructures informatiques au niveau national.

Afin de renforcer la sécurité informatique, un cadre réglementaire et un dispositif de formation professionnelle ont été mis en place, et les organismes publics responsables ont coordonné leurs travaux, entre autres pour rendre plus efficace leur coopération avec l'équipe d'intervention informatique d'urgence d'Ukraine (CERT-UA) et le Forum des équipes de veille et de réponse aux incidents de sécurité informatique, organisation internationale accréditée.

Conformément à la législation ukrainienne, l'équipe d'intervention fonctionne au sein du service public chargé des communications spécialisées et de la protection de l'information et coordonne, quel qu'en soit le régime de propriété, les activités des entreprises, des établissements et des organisations visant à prévenir, analyser et éliminer les conséquences découlant d'actes illicites perpétrés à l'encontre des ressources informatiques nationales dans les systèmes informatiques et télématiques.

En outre, l'équipe coopère avec les organes et organismes étrangers et internationaux compétents, et les obligations qu'elle doit remplir vis-à-vis de ses homologues étrangers [membre de plein droit du Forum des équipes de veille et de réponse aux incidents de sécurité informatique et participation au Partenariat multilatéral international contre les cybermenaces (UIT-IMPACT)] alimentent la coopération internationale en matière de sécurité informatique.

Conformément à la loi amendant la loi portant ratification de la Convention sur la cybercriminalité, le Ministère des affaires intérieures est l'autorité compétente en charge de la création et du fonctionnement d'un réseau permanent d'intervention d'urgence, fournissant des services d'enquête sur les délits relatifs aux systèmes et aux données informatiques, engageant des poursuites judiciaires à l'encontre de leurs auteurs et collectant des preuves sous forme électronique.

Le Ministère des affaires intérieures s'est doté d'une division administrative, le département chargé d'organiser le fonctionnement du réseau permanent d'intervention dans les cas de délit informatique, rattaché à la Direction de la lutte contre la cybercriminalité, et auquel il incombe d'effectuer les tâches et activités ci-après, qui consistent, entre autres, à lutter contre :

- Les attaques par déni de service;
- Les infractions commises par l'utilisation de cartes de paiement ou de leurs informations bancaires;
- Le piratage des sites bancaires offrant des services à distance à leurs clients;
- La diffusion de contenus illégaux (contrevenant au droit d'auteur) sur Internet;
- La diffusion sur Internet d'images à caractère pornographique, notamment celles qui mettent en scène des enfants;
- Les infractions relatives aux télécommunications;
- Les infractions relatives au piratage de réseaux satellites de diffusion de données;
- La fraude financière et toutes les autres formes de fraude commises sur Internet;
- Les infractions relatives au commerce électronique;

Il lui revient également d'organiser les travaux du réseau permanent d'intervention dans les cas de délit informatique.

Les travaux de mise à jour de la législation relative à la sécurité informatique se poursuivent afin que le cadre juridique réglementaire ukrainien soit conforme aux règles internationales en la matière.

Conformément au décret n° 1119 promulgué par le Président ukrainien le 10 décembre 2010, portant sur la décision prise par le Conseil national de sécurité et de défense le 17 novembre 2010 relativement aux défis et aux menaces auxquels l'Ukraine devait faire face en 2011, un projet de loi relatif à la sécurité informatique de l'Ukraine est en cours d'élaboration.

Les orientations prospectives de la politique nationale, prises conformément aux textes législatifs existants, sont les suivantes :

1) *En vertu des décrets ci-après promulgués par le Président ukrainien* : n° 1119, en date du 10 décembre 2010, relatif à la décision prise par le Conseil national de sécurité et de défense le 17 novembre 2010 relativement aux défis et aux menaces auxquels l'Ukraine devait faire face en 2011 (par. 4); n° 388, en date du 8 juin 2012, relatif à la décision prise par le Conseil national de sécurité et de défense le 25 mai 2012 relativement aux mesures de renforcement de la lutte antiterroriste en Ukraine (par. 1); n° 389, en date du 8 juin 2012, relatif à la décision prise par le Conseil national de sécurité et de défense le 8 juin 2012 relativement à la révision de la stratégie de sécurité nationale (par. 3.1.1, 3.3 et 4.3); n° 390, en date du 8 juin 2012, relatif à la décision prise par le Conseil national de sécurité et de défense le 8 juin 2012 relativement à la révision de la doctrine militaire ukrainienne (par. 7 et 19), il est prévu d'entreprendre les activités suivantes :

- Création d'un système national de cybersécurité;
- Création d'un système national unique de lutte contre la cybercriminalité;
- Élaboration et validation d'une liste de sites vitaux pour la sécurité et la défense nationales et revêtant une importance de premier plan dans la protection contre les attaques informatiques;
- Élaboration et présentation au Parlement ukrainien d'un projet de loi sur la cybersécurité nationale;
- Définition de la cybercriminalité en tant que l'une des principales menaces pesant sur la stabilité internationale et la sécurité nationale;
- Attribution d'une importance stratégique et d'un rôle essentiel dans la politique de sécurité nationale à l'élaboration des normes et des règles techniques relatives à l'informatique et aux communications et à leur harmonisation avec les normes en vigueur dans les pays de l'Union européenne;
- Définition du terme « cyberterrorisme »;
- Création à l'échelle du pays d'un mécanisme efficace d'intervention face aux nouveaux défis posés par la sécurité nationale (phénomènes et tendances susceptibles, lors de circonstances particulières, de menacer les intérêts nationaux) en matière d'utilisation de l'informatique dans le contexte de la mondialisation, notamment les « cybermenaces »;

- Assimilation des « attaques cybernétiques » visant des sites nucléaires, des usines chimiques, des complexes militaro-industriels et d'autres sites potentiellement dangereux à des agressions militaires, de nature à créer les conditions de déclenchement d'un conflit armé;

2) *Actes législatifs établis par le Conseil des ministres d'Ukraine* : Règlement n° 720-r en date du 22 août 2012, portant approbation d'un train de mesures en vue de la mise en œuvre du programme national annuel de coopération entre l'Ukraine et l'OTAN pour 2012, et instruction n° 24066/1/1-12 en date du 15 juin 2012, relative à la décision susmentionnée prise par le Conseil de sécurité et de défense nationale, entrée en vigueur par le décret n° 388 en date du 8 juin 2012, promulgué par le Président ukrainien, visant également à l'élaboration d'un acte législatif sur les questions relatives à la cybercriminalité;

3) *Les projets de loi portant amendement de certains actes législatifs relatifs à la cybersécurité nationale font l'objet d'un examen parlementaire*. Lesdits projets prévoient entre autres d'introduire dans le droit interne des notions telles que « sécurité cybernétique de l'État », « sites d'infrastructures clefs », « sites d'infrastructures informatiques clefs » et « espace cybernétique (cyberespace) », et de définir les menaces de nature cybernétique qui pèsent sur la sécurité nationale, les principales orientations de la politique de l'État et les fonctions des agents chargés d'assurer la sécurité nationale dans ce domaine.

3. Introduction de principes internationaux visant à renforcer la sécurité des systèmes informatiques et télématiques mondiaux

En Ukraine, le cadre législatif ukrainien relatif à la protection de l'information dans les systèmes informatiques et télématiques est conforme, tant par les principes que par l'approche, à la norme internationale ISO 15408, Critères d'évaluation pour la sécurité TI.

Étant donné que la criminalité informatique a dépassé les frontières nationales pour devenir un phénomène international, l'Ukraine a instauré une coopération régulière avec les forces de l'ordre d'autres pays.

Il convient également de souligner que l'Ukraine s'efforce d'œuvrer à la sécurité informatique à l'échelle internationale en exécutant les projets et les programmes de l'Organisation pour la sécurité et la coopération en Europe, de l'Assemblée parlementaire du Conseil de l'Europe, du Conseil de l'Europe, de l'OTAN dans le cadre de l'initiative Partenariat pour la paix, ainsi que par le biais d'accords bilatéraux.

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

Compte tenu du caractère transnational de la criminalité informatique, il est fondé de considérer opportun d'établir des principes internationaux visant à renforcer la sécurité des réseaux informatiques et télématiques, d'élaborer une politique internationale globale de sécurité et d'améliorer la connaissance des

formes sous lesquelles les menaces peuvent apparaître, les méthodes d'évaluation de celles-ci et les moyens permettant de les dépister.

L'élaboration et l'adoption d'instruments juridiques internationaux visant à définir précisément la terminologie relative au domaine est l'une des orientations de base que doit suivre la politique mondiale de sécurité informatique. En outre, il importe de définir le statut juridique du cyberespace et de donner une assise juridique aux compétences des États à l'égard des composants nationaux de cet espace (comme c'est le cas pour l'espace aérien ou l'espace maritime) et, par conséquent, de la réglementation des questions relatives à la cyberguerre, aux agressions cybernétiques, etc.

Il est essentiel que l'activité normative dans ce domaine se fonde sur une conception unifiée de la notion de cybercriminalité, ainsi que sur la codification exacte des actes qui y sont associés.

Afin de renforcer la sécurité informatique à l'échelle mondiale, la communauté internationale pourrait aussi prendre des mesures telles que l'harmonisation du cadre réglementaire de protection de l'information, la fixation, d'un commun accord, de critères et de méthodes d'évaluation de l'efficacité des systèmes et des moyens mis en œuvre en matière de sécurité informatique, la reconnaissance mutuelle des certificats d'origine en matière de protection de l'information et l'élargissement de la coopération en vue de régler les questions à caractère scientifique, technique ou juridique qui se posent dans le domaine de la sécurité informatique. Pour parvenir à de bons résultats, il serait également nécessaire de renforcer la coopération des forces de maintien de l'ordre chargées de prévenir et de réprimer les délits informatiques et d'engager des poursuites à l'encontre des contrevenants.