Nations Unies A/64/129/Add.1

Assemblée générale

Distr. générale
9 septembre 2009
Français
Original : espagnol/français

Soixante-quatrième session
Point 91 de l'ordre du jour provisoire*
Les progrès de l'informatique et de la télématique et la question de la sécurité internationale

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

Rapport du Secrétaire général

Additif**

Table des matières

Page

II. Réponses reçus des gouvernements 2
Cuba 2
Mali 6
Espagne 10

* A/64/150 et Corr.1
** Les renseignements contenus dans le présent document ont été reçus après la publication du rapport principal.

09-50576 (F) 180909 240909

II. Réponses reçues de gouvernements

Cuba

[Original : espagnol]
[2 juillet 2009]

Réponse à la résolution 63/37 : « Les progrès de l'informatique et de la télématique et la question de la sécurité internationale »

1. Cuba partage entièrement la préoccupation exprimée dans la résolution 63/37 concernant l'utilisation de la téléinformatique à des fins incompatibles avec la stabilité et la sécurité internationales et pouvant porter atteinte à l'intégrité des États, au détriment de leur sécurité dans les domaines tant civils que militaires. De plus, cette résolution souligne à bon droit la nécessité de prévenir l'utilisation de l'information ou des technologies de l'information à des fins criminelles ou terroristes.

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

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

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

5. Les gouvernements américains n'ont pas réparé le mal qu'ils ont pu faire à la paix et à la sécurité internationales, en créant des situations dangereuses comme l'usage d'un avion militaire pour transmettre des signaux de télévision vers Cuba sans son consentement. C'est là indigne d'un membre permanent du Conseil de sécurité des Nations Unies.

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

7. À la fin de mai 2009, on a compté un total de 1 924 heures de transmissions illégales hebdomadaires sur 30 fréquences des États-Unis vers Cuba. Plusieurs de ces émetteurs de radio appartiennent ou fournissent leurs services à des organisations liées à des éléments terroristes connus résidant en territoire américain

où ils agissent contre Cuba par des émissions où ils incitent au sabotage, aux attentats politiques, aux tueries et à d'autres actes prônés par le radioterrorisme.

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

- Les principes fondamentaux de l'Union internationale des télécommunications, énoncés dans le préambule de sa constitution, sur l'importance croissante des télécommunications pour le maintien de la paix et le développement économique et social de tous les États, afin de faciliter les relations pacifiques, la coopération internationale entre les peuples et le développement économique et social par le bon fonctionnement des télécommunications. Le contenu des émissions télévisées transmises par le Gouvernement des États-Unis vers Cuba a un caractère subversif, déstabilisateur et trompeur qui contredit ces principes;
- Les dispositions CS 197 et CS 198 de la Constitution de l'Union internationale des télécommunications, qui précisent que toutes les stations, quel qu'en soit l'objet, doivent être installées et exploitées de manière à ne pas causer de brouillages préjudiciables aux communications ou services de radiocommunication des autres États membres;
- L'Accord conclu à la neuvième session plénière de la Conférence mondiale des radiocommunications (CMR), tenue en novembre 2007, qui indique au paragraphe 6.1, alinéa g), qu'une station de radiodiffusion fonctionnant à bord d'un aéronef et émettant uniquement en direction du territoire d'une autre administration sans l'accord de celle-ci ne peut être considérée comme étant conforme au Règlement des radiocommunications;
- L'article 8, paragraphe 8.3, du Règlement des radiocommunications de l'Union internationale des télécommunications, qui indique que les fréquences attribuées et inscrites, avec reconnaissance internationale, doivent être respectées par les autres administrations quand celles-ci effectuent leurs propres attributions afin d'éviter un brouillage préjudiciable;
- L'article 42, paragraphe 42.4, du Règlement des radiocommunications de l'Union internationale des télécommunications, qui interdit aux stations d'aéronefs en mer ou la survolant d'effectuer tout service de radiodiffusion;
- L'avis du Comité du règlement des radiocommunications qui, à sa 35e séance en décembre 2004, a constaté le brouillage préjudiciable aux services cubains que ces transmissions causaient à 213 MHz et a demandé au Gouvernement des États-Unis d'Amérique de prendre les mesures voulues pour l'éliminer. De plus, depuis septembre 2006, ledit comité demande au Gouvernement des États-Unis d'Amérique quelles mesures il a prises pour éliminer le brouillage à 509 MHz, jusqu'ici sans recevoir de réponse. Le 20 mars 2009, la cinquantième réunion dudit comité a pris fin et, dans son résumé des décisions prises (document RRB09-1/5), elle rappelle encore l'illégalité des transmissions et demande au Gouvernement des États-Unis d'Amérique de prendre toutes les mesures nécessaires pour éliminer ces deux cas de brouillage des services de télévision cubains;
- Le paragraphe 23.3 de l'article 23 du Règlement des radiocommunications de l'Union internationale des télécommunications, qui limite les émissions

télévisées hors des frontières nationales. Un rapport de janvier 2009 publié par le General Accounting Office du Gouvernement des États-Unis reconnaît les violations des normes internationales et de la législation interne commises par le programme d'émissions de radio et de télévision du Gouvernement des États-Unis vers Cuba.

9. De plus, Cuba rappelle que la Conférence mondiale des radiocommunications (CMR-07) qui s'est tenue à Genève du 22 octobre au 16 novembre 2007, a adopté des conclusions qui qualifient de non conformes au Règlement des radiocommunications les émissions à partir d'aéronefs depuis les États-Unis vers Cuba. Les conclusions convenues en plénière ont dit textuellement ce qui suit : « Une station de radiodiffusion fonctionnant à bord d'un aéronef et émettant uniquement en direction du territoire d'une autre administration sans l'accord de celle-ci ne peut être considérée comme étant conforme au Règlement des radiocommunications. » Ces conclusions ont été convenues au niveau plénier de la Conférence et elles ont donc force légale pour les travaux de l'Union internationale des télécommunications. C'est ainsi que la Conférence mondiale des radiocommunications a entériné la déclaration faite en 1990 par ce qui était le Comité international d'enregistrement des fréquences et selon laquelle les transmissions de télévision à bord d'un aérostat avec des programmes dirigés vers le territoire national cubain contreviennent au Règlement.

10. L'hostilité du Gouvernement des États-Unis d'Amérique envers Cuba s'est manifestée par le blocus économique, commercial et financier imposé depuis près de 50 ans et qui affecte aussi l'informatique et la télématique comme on le voit dans les exemples suivants parmi bien d'autres :

- Cuba n'a pas le droit d'accéder aux services qu'offrent un grand nombre de sites Web sous prétexte que la liaison émane du domaine cubain *.cu* de l'Internet;
- Sans préavis, on a bloqué les domaines *.com* liés à Cuba, mesure prise récemment par le Bureau du contrôle des avoirs étrangers;
- Autre exemple : l'annonce faite en mai 2009 par le consortium technologique Microsoft de suspendre son service de conversation « Windows Live Messenger IM » pour Cuba et d'autres pays « pour se conformer à la législation des États-Unis ». Lorsqu'on veut utiliser cet outil, on lit donc ceci : « Microsoft a supprimé le service de Windows Live Messenger IM pour les usagers des pays visés par l'embargo des États-Unis; Microsoft n'offrira donc plus de services de Windows Live dans votre pays »;
- D'autres pages Web ont refusé l'accès à partir du domaine *.cu*; Cisco Systems (http://tools.cisco.com/RPF/register.do) pour les technologies de branchement, les routeurs pour les serveurs d'accès à l'Internet, y compris le matériel de vidéo numérique; SolidWorks (http://www.solidworks.com/sw/termsofuse.htlm) pour les systèmes automatisés de conception; et Symantec (http://www.symantec.com/about/profile/policies/legal) pour les logiciels de protection antivirus;
- Avec un cynisme et une hypocrisie sans exemple, les États-Unis accusent mensongèrement Cuba d'interdire à ses citoyens l'accès au réseau mondial, alors qu'en réalité c'est Cuba qui, en raison des lois du blocus imposé par les États-Unis, ne peut se brancher sur les câbles à fibre optique qui entourent

l'archipel cubain, ce qui l'oblige à payer les frais élevés des services de satellites;

- L'entreprise de télécommunications de Cuba SA (ETECSA) a subi des pertes de 53 769,80 dollars jusqu'à décembre 2008 en raison essentiellement de son exclusion du marché des États-Unis pour acheter du matériel spécialisé. Cela l'oblige à passer par des intermédiaires qui majorent énormément le prix des produits nécessaires pour offrir leurs services.

11. Cette attitude des États-Unis sape l'esprit, la volonté et les résultats qui ont prévalu entre les nations du monde entier lorsqu'elles se sont réunies en Suisse et à Tunis pour le Sommet mondial sur la société de l'information (SMSI) qui a exhorté énergiquement les États à adopter, dans la construction de la société de l'information, les dispositions nécessaires pour éviter, et pour s'abstenir d'adopter, toutes mesures unilatérales contraires au droit international et à la Charte des Nations Unies et de nature à nuire au développement économique et social complet de la population des pays affectés, et à réduire le bien-être de leurs citoyens.

12. La douzième session de la Commission de la science et de la technologie au service du développement, tenue à Genève du 25 au 29 mai 2009, a, par son analyse des progrès réalisés dans la mise en œuvre et le suivi des résultats du SMSI, offert un important auditoire pour réitérer la condamnation par Cuba de la politique de blocus menée par le Gouvernement des États-Unis et notamment de l'application de mesures coercitives unilatérales contre le développement des technologies des communications et l'accès à l'information, ainsi que l'exécution d'une politique d'agression contre le spectre radioélectronique de Cuba, contrairement aux dispositions adoptées lors des deux phases dudit sommet.

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

14. Cuba appuie résolument cet exercice à l'Assemblée générale des Nations Unies et elle s'est donc jointe aux 178 États Membres qui ont voté pour la résolution 63/37, contrairement à la position prise encore par les États-Unis d'Amérique, seul pays à voter non.

15. Cuba continuera de concourir au maximum au développement mondial pacifique de l'informatique et de la télématique et à leur emploi pour le bien de toute l'humanité, et elle est prête à collaborer avec les autres pays, y compris les États-Unis d'Amérique, pour surmonter les obstacles à la réalisation de ces objectifs.

Mali

[Original : français]
[9 juillet 2009]

Vues et observations relatives à la mise en œuvre de la résolution portant sur les progrès de l'informatique et de la télématique et la question de la sécurité internationale

Problèmes généraux en matière de sécurité de l'information

1. Le déni de service, qui vise à stopper le fonctionnement d'un système informatique, et l'intrusion en vue de détourner des informations sont les principales formes d'attaque des systèmes informatiques.

2. Les menaces pesant sur les systèmes gouvernementaux ou d'entreprises sensibles touchent l'intégrité, la confidentialité ou la disponibilité de l'infrastructure d'information essentielle.

3. On peut citer, entre autres :

- Les menaces orchestrées par un gouvernement étranger, un groupe terroriste ou des extrémistes ayant un mobile politique;
- Les menaces aux fins d'espionnage, de sabotage, d'ingérence étrangère ou de violence à caractère politique (terrorisme).

4. L'usage des technologies informatiques apparaît comme une alternative au recours à des méthodes plus traditionnelles, telles que la destruction, le brouillage par rayonnement électromagnétique, l'intrusion physique ou le contrôle de sources de renseignement internes.

5. Les attaques informatiques peuvent viser aussi bien des particuliers que des entreprises ou des institutions publiques. En ce qui concerne celles mettant en cause la défense ou la sécurité nationale, les services de l'État, les opérateurs d'importance vitale et les entreprises intervenant dans des domaines stratégiques ou sensibles sont particulièrement concernés. Toutefois, ces attaques n'ont pas le même type de conséquences selon qu'elles visent des sites ou services accessibles au public, des systèmes opérationnels ou plus directement des personnes détentrices d'informations sensibles.

6. L'identification de l'origine d'une attaque informatique est particulièrement difficile. Les procédés utilisés font le plus souvent appel à une succession d'ordinateurs pouvant être situés dans plusieurs pays différents. Remonter la chaîne des machines impliquées supposerait des enquêtes extrêmement longues, tributaires des aléas de la coopération judiciaire internationale. Les méthodes de dissimulation sont nombreuses et vont du détournement d'ordinateurs à l'insu de leur propriétaire au recours à des ordinateurs publics et anonymes, comme ceux situés dans les cybercafés.

7. Malgré tout, la plupart des services gouvernementaux et des observateurs discernent, derrière ces attaques, des groupes de pirates informatiques dont les méthodes semblent de plus en plus perfectionnées.

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

a) Au plan national

8. Actuellement, le Mali ne dispose pas d'une législation en matière de sécurité de l'information.

9. La mise en place d'un cadre juridique et réglementaire est l'un des axes prioritaires du plan stratégique national des technologies de l'information et de la communication adopté par le Gouvernement en juin 2005.

10. Le Gouvernement a obtenu de l'Association internationale de développement (IDA) un crédit (4 033 MLI) pour financer le Projet d'appui à la croissance et il se propose d'en utiliser une partie pour réaliser une consultation relative à l'assistance technique pour la préparation du cadre juridique et réglementaire des TIC au Mali.

11. La sélection de consultants par les emprunteurs de la Banque mondiale s'est traduite par la sollicitation de manifestations d'intérêt n° 001/2009/SPM/UCP-PAC, conformément au cahier des charges élaboré en mai 2008 par l'Agence des technologies de l'information et de la communication (AGETIC).

12. Dans ce cadre juridique et réglementaire, il est prévu l'élaboration de textes législatifs sur les libertés, les affaires, le commerce électronique, la propriété intellectuelle, la sécurité et la confidentialité des données, les crimes et délits dans le cyberespace, le libre accès aux informations publiques et à celles constituant le patrimoine de l'humanité.

b) Les activités de coopération internationale pour le renforcement de la sécurité de l'information

13. Les attaques informatiques s'affranchissent des frontières et peuvent être dirigées simultanément contre plusieurs États. La surveillance des réseaux et la mise au point des réactions en cas d'incident justifient une coopération et une assistance internationales. De manière plus générale, la protection des systèmes d'information face aux activités illégales constitue aujourd'hui une préoccupation commune à de nombreux États.

14. Le Mali, par ailleurs, opte pour une approche régionale de l'évolution de la réglementation du secteur des télécommunications, ce qui a conduit à la ratification des directives de l'Union économique et monétaire ouest-africaine (UEMOA) en 2006 et des actes additionnels de la Communauté économique des États de l'Afrique de l'Ouest en 2007.

15. L'Union internationale des télécommunications travaille à l'établissement d'un cadre international pour la promotion de la cybersécurité (Programme mondial cybersécurité) auquel l'État malien s'intéresse particulièrement. Cette promotion de la cybersécurité a conduit à la création d'un groupe d'experts de haut niveau chargé de proposer une stratégie à long terme englobant les mesures légales, les mesures techniques visant à remédier aux failles des produits logiciels, ainsi que la prévention et la détection des attaques informatiques et la gestion des crises.

La teneur des principes internationaux susceptibles de renforcer la sécurité de la téléinformatique

16. La sécurité de l'information au niveau international devrait reposer sur le droit international existant (*jus ad bellum*), qui définit comment contrer les menaces contre la paix et la sécurité internationales, et sur le droit international humanitaire (*jus in bello*), qui porte sur les méthodes et les moyens de guerre, la protection des États qui ne sont pas parties au conflit, ainsi que sur les personnes et biens qui sont ou pourraient être touchés par lui.

17. La Charte des Nations Unies est la pierre angulaire du droit international s'agissant du maintien de la paix et de la sécurité internationales.

18. L'ensemble des spécialistes du droit international reconnaissent que ces règles instaurent un mécanisme universel de sécurité pour préserver la paix et la sécurité internationales. Alors que les technologies de l'information et de la communication sont désormais conçues ou employées comme moyens de destruction (autrement dit les « armes de l'information ») et que la communauté internationale n'a pas encore convenu de la place de la sécurité de l'information dans le droit international existant, la Charte des Nations Unies pourrait être interprétée de façon à laisser aux acteurs internationaux une liberté importante d'utiliser les technologies de l'information et de la communication pour mener des actions agressives et régler des conflits et différends internationaux.

19. Cette situation surprenante découle du fait que les actions hostiles dans le domaine de l'information ne sont pas encore envisagées explicitement par le droit international sur le même plan que des actions hostiles avec des armements classiques – même si l'interconnectivité du monde d'aujourd'hui et sa dépendance à l'égard des technologies de l'information et de la communication signifient qu'une telle attaque serait aussi dévastatrice qu'une attaque classique, voire peut-être plus. Les difficultés sont exacerbées par l'absence d'interprétations communément admises de notions telles que l'« acte d'agression » (art. 1), la « force » (art. 2, al. 4) et l'« agression armée » (art. 51) s'agissant de la sécurité de l'information.

20. La résolution 3314 (XXIX) de l'Assemblée générale, en date du 14 décembre 1974, définit l'acte d'agression.

21. Même si cette résolution n'a pas été adoptée par consensus, ses dispositions indicatives donnent au Conseil de sécurité et à tous les membres de la communauté internationale des critères pour déterminer un acte d'agression.

22. L'utilisation d'une arme de l'information peut être interprétée comme un acte d'agression si l'État victime a des raisons de penser que l'attaque a été menée par les forces armées d'un autre État et visait à perturber le fonctionnement d'installations militaires, à détruire des capacités de défense ou économiques, ou à violer la souveraineté de l'État sur un territoire particulier.

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

23. Afin de renforcer la sécurité de l'information à l'échelon mondial et de faire face à la menace d'utilisation des technologies de l'information et de la

communication à des fins hostiles, la communauté internationale se doit d'accentuer son intervention dans certains domaines tels que :

a) L'accompagnement des États dans la sensibilisation et la responsabilisation des différents acteurs (administrations, entreprises et utilisateurs) à la sécurité des systèmes d'information; dans ce contexte, une large place doit être attribuée à la coordination des politiques entre les États en termes de soutien à la base industrielle et technologique des produits sécurisés. Une place prépondérante doit être accordée également à la collaboration entre États et secteurs privés;

b) Le renforcement de la capacité des États en mettant à leur disposition des moyens humains et l'expertise technique nécessaires pour la surveillance, et donc la détection, des flux anormaux par lesquels transitent les attaques informatiques;

c) La réorganisation des politiques des différentes institutions internationales qui opèrent dans le domaine de la sécurité des systèmes d'information en attribuant à chacune des compétences spécifiques;

d) L'instauration d'indicateurs dans le domaine de la sécurité informatique pour aider les nations à mieux gérer les infrastructures des TIC. Ces indicateurs peuvent concerner, entre autres, les aspects suivants :

- Restauration des données en cas de désastre;
- Utilisation des normes;
- Contrôle de performance (benchmarking);
- Transfert électronique;
- Collaboration avec Interpol;
- Plate-forme d'accès.

Conclusion

24. À l'issue de nos observations, il apparaît que les questions sur la sécurité informatique et l'utilisation des technologies de l'information et de la communication à des fins malveillantes inquiètent de plus en plus. Ces technologies offrent certes des avantages innombrables mais elles peuvent engendrer des désastres aux conséquences incalculables compte tenu de leur développement effréné.

25. Les questions juridiques posées par leur développement n'ont jusqu'à présent pas trouvé de réponses satisfaisantes à cause des diverses réglementations souvent mal adaptées.

26. Il revient donc aux États de veiller à la construction harmonieuse de ces outils pour garantir une meilleure ascension vers une société de l'information mieux sécurisée.

Espagne

[Original : espagnol]
[8 juillet 2009]

Position de l'Espagne sur les progrès de l'informatique et de la télématique et la question de la sécurité internationale

Introduction

1. La sécurité de l'information est un aspect essentiel de la société de l'information. Les progrès technologiques ont permis l'accroissement constant et accéléré des capacités de traitement et de stockage de l'information sous de multiples formats; par ailleurs, dans le domaine des communications, on constate la très forte augmentation de la largeur des bandes disponibles, ce qui permet de transmettre et de recevoir d'énormes quantités d'information pratiquement en temps réel et sans exiger d'infrastructures particulièrement complexes.

2. Mais, tout en améliorant l'accès à l'information de tous types, ces progrès technologiques facilitent le recours ou l'accès à celle-ci à des fins illicites, à commencer par l'emploi des systèmes télématiques et informatiques à des fins hostiles ou criminelles, y compris les actes de terrorisme ou les agressions, entre États ou entre acteurs transnationaux.

3. L'an dernier, on a constaté la tendance croissante à ce que l'Internet serve à des organisations criminelles et en particulier aux groupes terroristes, qui exploitent deux de ses caractéristiques : son universalité et l'anonymat qu'il peut garantir.

4. 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 cadre 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.

Usage de l'Internet à des fins terroristes

5. Actuellement, les principales menaces dans l'emploi de l'Internet par des organisations terroristes sont les suivantes :

a) Usage offensif pour attaquer les systèmes informatiques d'infrastructures primordiales ou l'infrastructure même de l'Internet. Les attaques de ce type sont relativement fréquentes dans le cadre de la délinquance ordinaire mais l'attaque subie par l'Estonie en 2007 a démontré que même les structures d'information d'un État peuvent en être victimes. On observe, directement liés à ce type de menace, l'augmentation considérable des logiciels nuisibles apparus depuis deux ans et les « botnets », ou réseaux d'ordinateurs « zombies » qui servent à attaquer les systèmes informatiques;

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

- Activités de communication. L'usage du Web remplace les communications des organisations criminelles faites par d'autres moyens comme la téléphonie à fil ou portable. Les instruments les plus utilisés pour communiquer par

l'Internet sont le courrier électronique, les programmes de messagerie instantanée et les forums;

- Diffusion de propagande et de documentation liées aux activités terroristes. Il existe actuellement des milliers de sites Web liés aux activités terroristes ou qui incitent à la violence, tendance qui s'est amplifiée avec l'apparition du phénomène des « blogs ». Or empêcher cet usage du Web par les organisations terroristes est assez compliqué car ces sites migrent très facilement. Il s'agit d'un phénomène transnational car le pays où se trouve le serveur contenant la page et à partir duquel celle-ci est administrée peut être bien distinct de celui où opère l'organisation terroriste en question;
- Activités de recrutement. Il arrive que l'Internet serve aux activités de racoleurs, surtout par les forums et les programmes de messagerie instantanée;
- Financement. L'Internet offre aux organisations terroristes la possibilité de mener des activités de collecte de fonds. Il est intéressant de noter que ces organisations peuvent ainsi participer à la commission de fraudes pour collecter des fonds;
- Diffusion de manuels d'entretien. Par l'Internet, les organisations terroristes diffusent des manuels sur les techniques du terrorisme, la fabrication d'explosifs ou l'emploi des armes;
- Mine d'informations pour commettre des attentats. L'Internet constitue une source d'information très riche qui, dans beaucoup de cas, sert aux organisations terroristes pour se renseigner sur leurs objectifs.

Mesures prises dans le cadre national pour lutter contre l'usage de l'Internet par les organisations terroristes

Mesures législatives

6. L'Espagne a fait un gros effort législatif ces dernières années, et surtout en 2007, en introduisant dans son système 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 espagnole. On a élaboré une vaste législation et des normes comportant tant des aspects purement nationaux que des directives de l'Union européenne visant à atteindre ces objectifs selon des critères nouveaux de sécurité de l'information où, pour atteindre un niveau raisonnable de protection tout en respectant la confidentialité de l'information, on s'applique avant tout, dans la plupart des cas, à en préserver l'intégrité et la disponibilité. À signaler notamment (ordre chronologique) :

- La loi organique 5/1992 du 29 octobre (et les mesures consécutives) qui réglemente le traitement automatisé des données à caractère personnel, inspirée par l'idée d'instaurer des mécanismes préventifs des atteintes à la vie privée résultant du traitement de l'information;
- La loi organique 15/1999 du 13 décembre (et les mesures consécutives) qui protège les données à caractère personnel en visant dans leur traitement à garantir et à protéger les libertés publiques et les droits fondamentaux des personnes physiques, et notamment leur honneur et leur intimité personnelle et familiale;

- Le décret-loi royal 14/1999 du 17 septembre sur la signature électronique, adopté afin de favoriser l'incorporation rapide des nouvelles technologies de sécurité des communications électroniques dans l'activité des entreprises, des citoyens et des administrations, qui a introduit dans la loi espagnole la directive 1999/93/CE du Parlement européen et du Conseil (13 décembre 1999) par laquelle a été créé un cadre communautaire pour la signature électronique. La loi 59/2003 du 19 décembre sur la signature électronique met à jour ce cadre en le modifiant en fonction de l'expérience acquise depuis son entrée en vigueur;

- La loi 11/2002 du 6 mai, réglementant le Centre national des renseignements (CNI) et, par la suite, le décret royal 421/2004 du 12 mars portant règlement du Centre national de cryptologie, textes par lesquels le CNI est notamment chargé de coordonner les actions des différents organismes de l'Administration qui utilisent des moyens et procédures de chiffrage, de garantir la sécurité des technologies de l'information dans ce domaine et de veiller au respect des normes relatives à la protection de l'information classifiée;

- La loi 34/2002 du 11 juillet sur les services concernant la société de l'information et le commerce électronique. Elle a pour objet d'introduire dans l'ordre juridique espagnol la directive 2000/31/CE du 8 juin, relative à certains aspects des services concernant la société de l'information, en particulier le commerce électronique sur le marché intérieur (directive sur le commerce électronique). De même, elle introduit en partie la directive 98/27/CE du Parlement européen et du Conseil (19 mai), relative aux actions en cessation en matière de protection des intérêts des consommateurs, en réglementant, conformément à ce qu'elle prescrit, l'action en cessation contre les conduites qui contreviennent à cette loi;

- La loi 32/2003 du 13 novembre sur les télécommunications, qui réglemente l'exploitation des réseaux et la prestation des services de communication électronique;

- La loi 59/2003 du 19 décembre sur la signature électronique, déjà citée;

- La loi 11/2007 du 22 juin, sur l'accès électronique des citoyens aux services publics, qui réglemente la communication par l'emploi et l'application des techniques et moyens électroniques, informatiques et télématiques existants entre les citoyens et les administrations;

- La loi organique 10/2007 du 8 octobre, réglementant la base de données policières sur les identifiants obtenus à partir de l'acide désoxyribonucléide (ADN), portant création d'une base de données où, chose unique, figurent les fichiers des forces et des organes de sécurité de l'État dans lesquels sont stockées les données d'identification obtenues à partir des analyses d'ADN réalisées dans le cadre d'une enquête criminelle ou dans l'identification des cadavres ou des personnes disparues;

- La loi 25/2007 du 18 octobre, sur la conservation des données relatives aux communications électroniques et aux réseaux publics de communications, qui aide aux enquêtes dans ce domaine;

- Le décret royal 1720/2007 du 21 décembre, approuvant le règlement d'application de la loi organique 15/1999 du 13 décembre, sur la protection des données à caractère personnel;
- La loi 56/2007 du 28 décembre, sur les mesures d'encouragement à la société de l'information;
- La qualification pénale des crimes cybernétiques suivants concernant les activités des organisations terroristes sur l'Internet :
  - Sabotages informatiques (art. 264 du Code pénal);
  - Menaces (art. 169 et suiv. du Code pénal);
  - Apologie et éloge du terrorisme (art. 578 du Code pénal).

Autres mesures

- Création de groupes de police chargés de lutter contre l'usage de l'Internet par les groupes criminels
- Participation au projet « Check the Web » élaboré par EUROPOL
- Création d'un centre de réponse rapide CERT pour améliorer la sécurité des systèmes informatiques des administrations
- Création du Centre national de protection des infrastructures primordiales

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

- L'usage de l'Internet par les organisations terroristes est un phénomène transnational qui exige dans de nombreux cas une enquête commune dans différents pays. Cela étant, les enquêtes et la prévention visant les activités terroristes sur l'Internet dépendent dans une large mesure de l'existence d'accords internationaux et d'autres outils de coopération internationale. À cet égard, une harmonisation législative s'impose pour lutter efficacement contre la présence de ces groupes criminels sur le Web. La collaboration policière internationale est essentielle aussi car la rapidité est cruciale dans ce type d'enquête en raison de la fugacité des preuves électroniques.
- Impliquer le secteur privé dans la lutte contre la cyberdélinquance. Le concours du secteur privé est essentiel car la majorité des services d'Internet est entre ses mains. Il consacre beaucoup de temps à faire face aux menaces sur l'Internet et ses connaissances et son expérience pourront être très utiles à cet égard.
- Faire prendre conscience à l'usager de la nécessité de veiller à la sécurité de ses systèmes informatiques. Si ce problème est mieux compris, on verra moins d'ordinateurs utilisés par les cyberdélinquants dans leurs activités, notamment celles concernant les « botnets ».
- S'agissant des mesures que la communauté internationale pourrait adopter pour renforcer la sécurité de l'information à l'échelle mondiale, il faudrait parvenir à la signature d'une convention entre États (analogue à la Convention internationale pour la sauvegarde de la vie humaine en mer ou comparable), par laquelle les États s'engageraient à unifier leurs législations pour permettre

la poursuite des délits dans le Web, en évitant dans la mesure du possible que l'anonymat, l'absence de législation et les intérêts économiques fassent du Web le creuset idéal pour la délinquance et le terrorisme. Tout cela devrait se faire sans nuire à la liberté de l'information ni au libre accès à celle-ci.

- Assouplir les procédures de coopération judiciaire et policière internationale pour pouvoir poursuivre les infractions pénales avec rapidité et efficacité, compte tenu du caractère diffus de l'Internet et de la fugacité des registres de branchement, selon la législation de chaque pays.

7. En conclusion, la communauté internationale devrait adopter les mesures de protection de l'information jugées nécessaires à partir d'une vision stratégique unitaire et, si possible, en créant une direction unique qui fixerait des normes et des critères pour tous les pays, établirait un ensemble équilibré et complet de mesures spécifiques de protection et permettrait l'harmonisation des politiques et des actions des différentes organisations nationales et internationales impliquées.