Nations Unies A/64/129

Assemblée générale

Distr. générale
8 juillet 2009
Français
Original : anglais/espagnol/russe

Soixante-quatrième session
Point 90 de la liste préliminaire*
Les progrès de l'informatique et de la télématique et la question de la sécurité internationale

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

Rapport du Secrétaire général

Table des matières

* A/64/50.

09-39634 (F) 310709 310709

I. Introduction

1. Au paragraphe 3 de sa résolution 63/37, l'Assemblée générale a invité tous les États Membres à continuer de communiquer au Secrétaire général leurs vues et observations sur les questions suivantes :

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

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

c) La teneur des principes visés au paragraphe 2 de la résolution;

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

2. Comme suite à cette demande, une note verbale a été adressée aux États Membres le 27 février 2009 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

Brésil

[Original : anglais]
[11 juin 2009]

1. L'information et les télécommunications constituent un élément essentiel des sociétés modernes, qui en sont largement tributaires. Aujourd'hui, presque aucune activité n'est possible si ces services ne sont pas constamment disponibles, ce qui en fait des ressources extrêmement précieuses qui revêtent une importance capitale pour la richesse et la prospérité des nations.

2. Les progrès technologiques qui ont rendu ce scénario possible ont également soulevé un certain nombre de problèmes dans le contexte de la sécurité internationale. Comme les sociétés dépendent de plus en plus de la disponibilité de l'information et de l'infrastructure des télécommunications, il est apparu de nouvelles vulnérabilités qui peuvent être exploitées à des fins militaires ou aux fins d'activités criminelles ou terroristes.

3. Une telle exploitation de l'informatique et de la télématique peut paralyser l'activité des entreprises privées, des banques, des bourses et des institutions gouvernementales. L'interconnexion croissante des réseaux de communication, bien qu'indubitablement bénéfique, donne naissance à toute une série de problèmes nouveaux auxquels les États doivent parer aux échelons aussi bien national qu'international.

4. L'informatique et la télématique modernes, outre qu'elles ont créé des vulnérabilités nouvelles, représentent simultanément une arme qui peut être utilisée comme moyen de guerre électronique. Il existe déjà des forces armées nationales dotées d'unités militaires spécialement formées et équipées pour pouvoir neutraliser, voire détruire, l'infrastructure critique d'un autre pays en envahissant ou sabotant ses réseaux informatiques. Selon l'objectif visé et les moyens employés, les effets

de telles attaques peuvent aller d'une neutralisation des systèmes d'armes ou de senseurs de l'ennemi à des perturbations cataclysmiques des réseaux de distribution d'énergie à l'échelle du pays tout entier.

5. Cette forme d'attaque est d'autant plus efficace que l'acquisition des moyens requis ne suppose qu'un investissement relativement modeste. Aussi la guerre électronique risque-t-elle fort de devenir bientôt le prélude des conflits militaires entre États. Le risque existe également que les mêmes tactiques soient utilisées par des individus ou des organisations à des fins terroristes.

6. Conscient de l'importance que cette question revêt pour le maintien de la paix et de la sécurité internationales, le Brésil suggère d'aborder la question sous deux angles différents. Premièrement, la communauté internationale devrait s'efforcer de mettre au point des mécanismes appropriés pour contrer les activités criminelles et terroristes faisant intervenir l'informatique et la télématique. Séparément mais simultanément, elle devrait étudier l'impact des nouveaux moyens de guerre électronique et, le cas échéant, la nécessité d'élaborer des instruments juridiques internationaux pour mettre en place des régimes de désarmement et de non-prolifération de nature à parer aux multiples risques inhérents à ces moyens de guerre.

7. Par ailleurs, l'utilisation qui peut être faite de ces moyens par des criminels et des terroristes devrait être discutée au sein des instances appropriées, et l'Organisation des Nations Unies devrait jouer le rôle qui lui revient en aidant les États Membres, selon que de besoin, à œuvrer à la réalisation des objectifs ci-après, entre autres :

- Établissement de mécanismes d'intervention et de réseaux de secours en vue de protéger l'infrastructure critique;
- Examen de la structure des réseaux, analyse des interdépendances et notification des méthodes de protection les plus efficaces;
- Établissement d'une étroite coopération entre les secteurs public et privé afin de garantir le degré voulu de sécurité de l'information échangée entre les organisations;
- Établissement de systèmes de protection en vue d'éviter ou de minimiser les effets d'attaques informatiques;
- Mise au point d'outils et de mesures permettant aux autorités d'identifier l'origine des attaques informatiques;
- Organisation d'un débat sur l'opportunité et la nécessité de conclure des instruments internationaux juridiquement contraignants contre la cybercriminalité;
- Homologation d'institutions nationales chargées d'évaluer et de tester le niveau de sécurité des systèmes d'information;
- Établissement de procédures de notification mutuelle des menaces d'attaques électroniques entre les autorités nationales compétentes;
- Nécessité d'éviter les mécanismes discriminatoires qui pourraient empêcher les pays d'avoir accès aux technologies de pointe dans les domaines de l'informatique et de la télématique;

- Réalisation d'activités d'éducation et de sensibilisation touchant l'importance de la sécurité informatique.

8. L'Organisation des Nations Unies devrait jouer un rôle de premier plan concernant l'utilisation de l'informatique et de la télématique comme moyens de guerre électronique dans les conflits entre États, en faisant porter tout particulièrement son attention sur les aspects suivants :

- Identification, caractéristiques et classification des moyens de guerre informatique;
- Identification et classification des armes informatiques et des moyens pouvant être utilisés comme armes informatiques;
- Établissement d'un code de conduite concernant l'utilisation des armes informatiques;
- Garantie de l'égalité de droits de tous les pays concernant la protection de leurs systèmes nationaux contre les attaques électroniques;
- Établissement d'un glossaire des Nations Unies contenant des définitions des principaux thèmes d'informatique et de télématique employés dans le contexte de la sécurité internationale.

Kazakhstan

[Original : russe]
[2 juillet 2009]

1. Le développement rapide des technologies de l'information et de la communication dans le monde entraîne des transformations profondes dans tous les secteurs de la vie des pays. Ainsi qu'il est dit dans la Charte d'Okinawa sur la société mondiale de l'information, les technologies de l'information sont l'un des facteurs déterminants à l'origine de la société du XXI^{e} siècle. Elles révolutionnent les modes de vie, l'éducation et le travail ainsi que les interactions entre les gouvernements et la société civile.

2. Dans les conditions actuelles de progrès rapides dans le domaine de la science et de la technique, on observe une nette tendance à l'informatisation et à la création de vastes réseaux de traitement des données. L'Internet touche à pratiquement tous les aspects de la vie de l'État et de la société et le nombre d'usagers ne cesse d'augmenter, faisant des ressources informationnelles, des systèmes de traitement des données et des réseaux informatiques le maillon le plus vulnérable de l'infrastructure de l'État.

3. Puisque l'Internet demeure un espace virtuellement libre, échappant pratiquement à tout contrôle, les organisations criminelles s'efforcent de mettre à profit les technologies modernes de l'information. De l'avis des experts de la Chambre de commerce internationale, le nombre d'infractions faisant appel à l'Internet augmente proportionnellement au nombre d'usagers. D'après les données d'INTERPOL, l'Internet est maintenant le domaine où la criminalité augmente le plus rapidement.

4. Les infractions se répartissent en trois catégories :

a) Infractions universelles contre les États et la société : celles qui mettent en danger la sécurité de l'État et de la société (en prônant le renversement de l'ordre établi, les violations de la souveraineté et de l'indépendance, les atteintes aux intérêts nationaux et en encourageant le terrorisme, le chauvinisme, la xénophobie, toutes les formes d'extrémisme et la discrimination fondée sur l'ethnicité, la race, la religion, le sexe, etc.);

b) Infractions civiles universelles : les atteintes aux droits et libertés de la personne (atteintes aux droits et aux libertés de la personne, calomnie, pressions, discrédit jeté sur les personnes, diffusion d'informations confidentielles, utilisation de l'Internet aux dépens d'autrui, falsification de documents, atteinte aux droits d'auteur, etc.);

c) Infractions additionnelles : les atteintes aux valeurs morales et à la décence (pornographie, pédophilie et autres formes de perversion sexuelle, toxicomanie, alcoolisme, etc.).

5. Ce phénomène est révélateur de l'insuffisance des lois nationales existantes applicables aux relations juridiques résultant de l'Internet et appelle une nouvelle réglementation supranationale. Au plan international, on n'a pas encore défini une démarche normative unique permettant d'identifier et d'évaluer les dangers pour la sécurité internationale de l'information ou les mécanismes de coopération internationale visant à écarter ces dangers. De plus, aucune des conceptions de la sécurité internationale de l'information proposées à ce jour par les différents pays n'a de portée universelle.

6. Cela s'explique par le fossé technologique qui sépare les pays développés et les autres, par des divergences politiques sous-jacentes, par des façons diamétralement opposées d'apprécier ce qui se passe dans le domaine de l'information et par d'autres facteurs.

7. Les documents internationaux existants – ceux de l'ONU et des organisations européennes, comme l'Organisation pour la sécurité et la coopération en Europe (OSCE) – privilégient les dangers liés à la criminalité ordinaire et au terrorisme, sans se soucier des risques d'utilisation illicite des technologies de l'information en période de conflit armé et de dominance dans le domaine informationnel, mettant en danger la souveraineté et l'identité nationales, ou encore des risques de catastrophe naturelle ou technologique compromettant notamment les structures informatiques nationales.

8. La protection contre ces risques pourrait être assurée à la fois par des accords conclus avec les partenaires militaires et politiques en matière de sécurité internationale de l'information et par des accords politico-juridiques sur le non-recours aux armes informationnelles et sur des mécanismes permettant de minimiser les effets négatifs d'un acte hostile et de rétablir le fonctionnement des structures nationales informationnelles, et autres.

9. Il convient de noter qu'un tel travail a déjà été entrepris, avec la participation du représentant de la République du Kazakhstan, dans le cadre aussi bien de l'Organisation du Traité de sécurité collective que de l'Organisation de Shangai pour la coopération, où des experts étudient la possibilité de conclure les accords intergouvernementaux appropriés. En exécution notamment du plan d'action visant à assurer la sécurité internationale de l'information, adopté à Bichkek le 16 août 2007 par les chefs d'État des États membres de l'Organisation de Shangai pour la

coopération, un groupe d'experts des États membres de l'Organisation a élaboré un projet d'accord international sur la coopération dans le domaine de la sécurité internationale de l'information, qui a été signé le 15 juin 2009 à Yekaterinburg à la réunion des chefs d'État des États membres de l'Organisation de Shangai pour la coopération.

10. On notera que cet accord est sans précédent dans la pratique mondiale et que, s'il est signé, il aura une grande importance internationale, puisqu'il est ouvert également à la signature d'autres États.

11. De plus, un groupe de travail intérimaire du Comité des secrétaires des conseils de sécurité de l'Organisation de sécurité collective travaille sur les questions de politique et de sécurité de l'information. Il a mis au point un programme d'action commune en vue de créer un système de sécurité de l'information des États membres de l'Organisation de sécurité collective.

12. Les États membres de l'Organisation de sécurité collective ont pris de concert des mesures préventives dans le cadre de l'opération Proxi reposant sur une vision unique des orientations de la coopération des organes de sécurité et des affaires intérieures (police).

13. Étant donné l'envergure et le caractère international de l'Internet, nous proposons que les États Membres de l'ONU élaborent et adoptent une convention internationale sur la sécurité de l'information, dont un élément essentiel serait la lutte contre la criminalité sur l'Internet.

14. Cet instrument devra être axé sur la coopération internationale mutuellement avantageuse dans le domaine de la sécurité de l'information et sur la prévention des conséquences géopolitiques négatives de la mondialisation de l'informatisation.

15. Il devra en outre prévoir des mécanismes organisationnels, techniques, programmatiques et sociaux de collecte de données et de leur utilisation, en vue de préserver le cadre constitutionnel, la souveraineté et l'intégrité territoriale de tous les États Membres de l'ONU, la stabilité politique, économique et sociale, la légalité et la primauté du droit ainsi que des mécanismes protégeant les droits et les libertés constitutionnelles de l'homme et du citoyen.

16. Au niveau national, un projet de loi tendant à modifier et compléter certains textes juridiques de la République du Kazakhstan sur des questions liées aux réseaux d'information et de communication a été rédigé et soumis au Sénat.

17. Il vise à renforcer les normes réglementant la diffusion d'informations sur le territoire de la République du Kazakhstan par ces réseaux.

18. Les organes de sécurité nationale font de gros efforts pour renforcer la sécurité de l'information et promouvoir la coopération internationale en la matière. Ils cherchent constamment à mettre en évidence et réprimer ces crimes informatiques au niveau international.

19. Ainsi, en 2008, le Comité national de sécurité, en coopération avec le Service fédéral de sécurité de la Fédération de Russie, a réprimé l'activité des gangs criminels organisés parmi les pirates informatiques qui extorquaient des sommes considérables pour cesser leurs attaques du type « déni de service » distribué sur les sites de sociétés offrant des services sur l'Internet.

20. Les recherches opérationnelles menées dans ce domaine révèlent l'apparition de nouvelles formes de criminalité sur l'Internet : extorsion, chantage, trafic d'êtres humains, proxénétisme, diffusion de pornographie, culte de la cruauté et de la violence, terrorisme et extrémisme.

21. Ainsi, en 2008, on a enregistré 45 cas de pornographie et il convient de noter à cet égard que la pornographie faisant intervenir des enfants est de plus en plus accessible sur l'Internet; on a enregistré un cas en 2005-2006, 7 en 2007 et 14 en 2008, notamment sur le réseau kazakh de l'Internet.

22. On notera par ailleurs que, faute d'une base juridique qui réglementerait l'information de façon rigoureuse, la lutte contre les attaques à la sécurité des informations et des technologies de pointe ne répond pas aux critères établis.

23. Les instruments juridiques normatifs qui existent dans ce domaine doivent être affinés, compte tenu des réalités d'aujourd'hui.

24. Il conviendrait, à notre avis, de s'appuyer sur l'expérience des pays qui ont des techniques de pointe, pour moderniser le droit pénal en prévoyant des peines plus sévères dans ce domaine.

25. Par ailleurs, étant donné le caractère transnational des crimes informatiques, les forces de l'ordre doivent sans cesse étendre leurs domaines de coopération pour réagir rapidement en cas d'attaque sur l'Internet. Les résultats de la coopération des forces de l'ordre du Kazakhstan avec des services spécialisés et les forces de l'ordre d'autres pays montrent que les attaques informatiques lancées depuis le segment kazakh de l'Internet se multiplient. Or les victimes se heurtent constamment à des problèmes de retards dans la communication d'informations concernant une attaque en cours, la République n'ayant pas de service spécial chargé de recevoir et transmettre aux organes gouvernementaux compétents les informations concernant des incidents informatiques qui soit comparable aux centres de sécurité de l'Internet existant dans d'autres pays.

26. Dans ce contexte, il nous paraît indispensable de créer, au sein des forces de police, des unités spécialisées dotées de moyens modernes chargées de la détection et de la répression des infractions en matière de sécurité de l'information.

27. Le Kazakhstan a également présenté sa candidature au groupe d'experts gouvernementaux qui sera créé conformément au paragraphe 4 de la résolution 63/57 de l'Assemblée générale intitulée « Les progrès de l'informatique et de la télématique et la question de la sécurité internationale ».

Liban

[Original : anglais]
[22 mai 2009]

1. Une nouvelle loi concernant le secteur des technologies de l'information et des communications doit être promulguée prochainement au Liban. Cette loi, dont les formalités d'approbation par la Chambre des députés touchent à leur fin, réglementera toutes les questions connexes, y compris la sécurité, ainsi que toutes les questions liées à la criminalité informatique.

2. Lorsque cette loi sera entrée en vigueur, le Ministère des télécommunications fera le nécessaire, en collaboration avec les autres ministères et toutes les administrations concernées, au sujet des points b), c) et d) [du paragraphe 3 de la résolution 63/37 de l'Assemblée générale – voir ci-dessus].

Lituanie

[Original : anglais]
[26 mai 2009]

1. La Lituanie attache une grande importance à la question de la sécurité de l'information aux échelons aussi bien national qu'international. La cybersécurité constitue un élément important de la sécurité nationale.

2. Il importe de promouvoir la coopération au plan international pour améliorer la protection des systèmes de communication et d'information ainsi que pour susciter une prise de conscience accrue à la question. La Lituanie se félicite de ce que la question de la sécurité de l'information commence à occuper une place plus large à l'ordre du jour d'organisations internationales comme l'Organisation des Nations Unies, l'Union européenne, l'Organisation du Traité de l'Atlantique Nord et l'Organisation pour la sécurité et la coopération en Europe et elle participe activement aux travaux qu'elles mènent dans ce domaine. Les institutions lituaniennes coopèrent étroitement avec leurs partenaires. La Lituanie est partie à la Convention de l'Europe sur la cybercriminalité depuis le 1er juillet 2004.

3. La Lituanie est l'un des sept pays membres de l'OTAN qui ont parrainé la création à Tallin (Estonie) du Centre pour la cyberdéfense en coopération (CDC), qui a été déclaré Centre d'excellence de l'OTAN le 14 mai 2008.

4. Le programme « L'Internet plus sûr », programme communautaire pluriannuel visant à promouvoir une utilisation plus sûre de l'Internet et des nouvelles technologies en ligne, a été adopté le 11 mars 2005 par Décision du Parlement européen et du Conseil. Ce programme a principalement pour but d'éduquer la société concernant les questions liées à une utilisation sûre de l'Internet et des services de téléassistance.

5. Pendant l'assemblée générale de l'Internet Hotline Providers Association (INHOPE), tenue les 28 et 29 mai 2008 à Dublin, la hotline lituanienne est devenue membre d'INHOPE.

6. Au plan national, la première évaluation de l'état de l'infrastructure informatique, réalisée en 2000, a marqué le début des efforts complexes entrepris pour garantir la sécurité des systèmes informatiques. L'évaluation a porté principalement sur le degré de compréhension des questions liées à la sécurité de l'information, les politiques existantes et le niveau de la cyberprotection dont jouissent les institutions de l'État.

7. Par sa résolution no 291 du 14 mars 2001, le Gouvernement lituanien a chargé le Ministère de l'intérieur de coordonner la sécurité des systèmes informatiques des institutions de l'État.

8. Plusieurs mesures ont été élaborées et appliquées en vue de sauvegarder la sécurité de l'information, conformément à la stratégie sur la sécurité des systèmes informatiques de l'État (jusqu'en 2004) et à la stratégie nationale relative à la

protection de la sécurité des systèmes informatiques et électroniques des institutions de l'État (jusqu'en 2008).

9. Le 17 juin 2008, le Premier Ministre a créé par décret un groupe de travail interinstitutions chargé des questions liées à la cybersécurité. Le 21 novembre 2008, le groupe de travail a soumis au Gouvernement un rapport contenant des propositions et recommandations visant l'amélioration de la cybersécurité en Lituanie.

10. Le Gouvernement lituanien se prépare à entreprendre prochainement la rédaction d'une loi sur les réseaux de communication électronique et de la sécurité de l'information ainsi qu'une nouvelle stratégie sur la sécurité des systèmes informatiques électroniques en vue de renforcer encore plus les capacités de l'État dans les domaines de la sécurité de l'information en général et de la cyberdéfense en particulier. La stratégie susmentionnée a notamment pour objectifs d'améliorer l'efficacité des structures institutionnelles qui constituent le cadre de défense contre les cyberattaques, de renforcer la sécurité et la résilience de l'infrastructure de transfert de données, de protéger efficacement l'infrastructure informatique critique contre les cybermenaces et d'assurer, au moyen d'audits aux deuxième et troisième degrés, le respect des politiques et des normes applicables.

11. Depuis 2005, l'Office lituanien de réglementation des communications a mené plusieurs études du réseau de communications électroniques et de la sécurité de l'information afin d'identifier les problèmes à résoudre. L'Office fait fonction d'équipe nationale d'intervention informatique d'urgence (CERT).

12. L'Équipe nationale lituanienne d'intervention informatique d'urgence (CERT-LT) est chargée de promouvoir la sécurité de la société de l'information en s'attachant à prévenir, surveiller et résoudre les incidents qui affectent la sécurité de l'information et à diffuser les informations concernant les menaces potentielles. Son nouveau site web www.cert.lt a été inauguré le 30 septembre 2008. Le 16 janvier 2009, l'Équipe nationale d'intervention informatique d'urgence est devenue membre accrédité du réseau Trusted Introducer, réseau des sites de confiance Computer Security Incident Response Team (CSIRT) et CERT d'Europe.

13. La Lituanie s'emploiera à veiller à ce que la communauté internationale continue de centrer son attention sur la question de la sécurité de l'information et redouble d'efforts dans ce domaine. Elle a l'intention de participer activement et de contribuer aux travaux futurs menés par la communauté internationale pour renforcer la sécurité de l'information.

Mexique

[Original : espagnol]
[8 juin 2009]

1. Les principaux problèmes de sécurité qui pourraient se poser tiennent à l'éventuelle vulnérabilité des systèmes d'information utilisés dans les programmes de défense des pays ainsi qu'au risque de détournement de l'informatique et des télécommunications par des terroristes à des fins violentes et dissuasives.

2. Dans ce contexte, attentif à l'évolution de la sécurité des télécommunications dans le monde, le Mexique a participé à l'Assemblée mondiale sur la normalisation

des télécommunications, qui s'est tenue en Afrique du Sud en octobre 2008, où il a présenté, avec d'autres membres de la Commission interaméricaine des télécommunications (CITEL) (le Canada, le Paraguay et l'Uruguay), une résolution invitant les universités à participer activement aux sessions afin de contribuer à ses travaux.

3. Par ailleurs, dans le contexte régional, le Mexique a assumé la vice-présidence de la XX^{e} réunion du Comité directeur permanent de la CITEL, et y a proposé aux États de la région un cours sur les interférences dans les systèmes satellitaires, organisé par la Commission fédérale des télécommunications. À cette occasion, les États ont convenu que la V^{e} Assemblée ordinaire de la CITEL aurait lieu au premier trimestre de 2010 au Mexique.

4. Parmi les mesures que le Mexique a prises pour renforcer la sécurité internationale dans le domaine de l'information et des communications, il convient de mentionner que le pays a à son actif son unité de police cybernétique qui, outre l'action de prévention des infractions informatiques et sur Internet, s'occupe de la prévention et de la gestion des cas signalés d'infractions commises contre des mineurs.

Serbie

[Original : anglais]
[9 juin 2009]

1. Il importe que les États consolident leurs normes juridiques concernant le cyberespace étant donné que celui-ci n'est plus limité au territoire d'un seul pays et que les individus et/ou groupes qui cherchent à déstabiliser les systèmes informatiques et télématiques ou à les utiliser à des fins qui ne sont pas les leurs peuvent, fréquemment, se trouver dans un pays autre que celui où survient un incident. La résolution adoptée constitue un premier pas et offre une base solide pour mettre en œuvre une approche équilibrée, fondée sur des recommandations, tendant à renforcer le cadre législatif au plan international en vue d'améliorer la sécurité internationale, d'une part, et de garantir le libre courant de l'information, de l'autre.

2. Des lois plus rigoureuses s'imposent, principalement au niveau de l'État. Ces lois doivent être adaptées aux compétences techniques et au niveau d'instruction des usagers et aller de pair avec une éducation continue des usagers et avec la création d'organismes spécialisés chargés de planifier, d'organiser et de contrôler les aspects techniques des systèmes de sécurité.

3. La sécurité de l'information, dans le contexte de la sécurité des systèmes informatiques et télématiques, appelle les observations suivantes :

Problèmes

- Il apparaît chaque jour de nouveaux types de programmes malveillants qui menacent la sécurité des systèmes informatiques et télématiques;
- Il a été enregistré de nombreuses tentatives de pénétration des sites Internet officiels du Ministère de la défense et des Forces armées de la République de Serbie;

- L'Internet est utilisé pour la propagation d'idées terroristes.

Procédures et coopération en matière de sécurité

- Des logiciels antivirus appropriés sont utilisés à tous les niveaux des systèmes informatiques et télématiques du Ministère de la défense et des Forces armées de la République de Serbie;
- Les sites Internet officiels du Ministère de la défense et des Forces armées de la République de Serbie sont continuellement protégés contre les attaques de pirates informatiques;
- L'on encourage la participation aux conférences et séminaires visant à susciter une prise de conscience accrue des dangers liés à la cybercriminalité et au cyberterrorisme.

Recommandations

Il conviendrait de créer une institution internationale chargée :

- D'évaluer les problèmes liés à la protection des données et des circuits de télécommunication;
- De suivre les facteurs qui peuvent constituer une menace dans les domaines du cyberterrorisme international et de la cybercriminalité;
- D'évaluer les problèmes que soulèvent la sécurité de l'information au plan international et les systèmes de télécommunication et de recommander des solutions;
- De concevoir des programmes d'éducation visant à sensibiliser aux dangers liés à la cybercriminalité et au cyberterrorisme; et
- D'organiser des échanges de connaissances et de données d'expérience aux niveaux intergouvernementaux.

Tadjikistan

[Original : anglais]
[20 mai 2009]

1. Les télécommunications sont considérées aujourd'hui comme un facteur important aussi bien de développement économique que de stabilité et de sécurité de tout pays.

2. Le Tadjikistan a créé les conditions voulues pour le développement des télécommunications en assurant la libre concurrence, en délivrant des licences à de nouveaux agents et prestataires de services et en mettant en place de nouveaux services.

3. Il est essentiel de veiller à assurer la sécurité du fonctionnement des infrastructures télématiques, d'améliorer la protection des réseaux informatiques des sociétés et de déjouer ainsi la diffusion des idéologies de terrorisme, d'extrémisme et de violence.

4. Le Tadjikistan est prêt à appuyer l'initiative proposée et à collaborer dans le domaine de la sécurité internationale de l'information.

Thaïlande

[Original : anglais]
[3 juin 2009]

Les problèmes généraux en matière de sécurité de l'information

1. Le monde est maintenant entré dans l'ère de la société de l'information et les technologies de l'information sont aujourd'hui utilisées pour faciliter, par exemple, les transactions financières et les échanges de nouvelles et d'informations. Néanmoins, ces technologies, tout en étant une source de bienfaits, présentent également des possibilités d'utilisation illégales et immorales par certains groupes et suscitent ainsi des problèmes comme le vol d'informations par le biais des systèmes informatiques, les cyberattaques, la falsification de documents électroniques, l'infiltration de bases de données gouvernementales en vue d'y voler des données personnelles et les atteintes à la vie privée. Il n'en demeure pas moins que les technologies de l'information et des communications (TIC) sont indispensables au développement économique de tous les pays. La complexité accrue de ces technologies, la pénurie de personnel suffisamment formé à la sécurité de l'information et l'insuffisance des ressources peuvent affecter la sécurité des systèmes et des réseaux informatiques, qui risquent ainsi de ne pas inspirer confiance, surtout dans les domaines comme la banque, le commerce électronique ou l'administration. Il faut par conséquent identifier et devancer les problèmes à prévoir afin d'adopter des mesures de protection et de sécurité pour parer à ces risques. À cette fin, les pays doivent coopérer afin de mettre au point des mesures visant à protéger la sécurité de l'information qui constituent une norme internationale devant être respectée par tous les pays.

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

2. Le Gouvernement royal thaïlandais a adopté un plan stratégique pour les années 2552-2554 de l'ère bouddhique (2009-2011) qui fait une place prioritaire à la politique de sécurité nationale. Le Gouvernement a adopté un certain nombre de mesures législatives afin de promouvoir la sécurité de l'information et d'éviter que les réseaux informatiques soient utilisés à des fins immorales ou à des fins affectant la sécurité nationale. Il a notamment été promulgué des lois concernant la cybercriminalité, les transactions électroniques, les signatures électroniques et les virements électroniques de fonds.

3. Le Ministère des technologies de l'information et des communications s'emploie activement à promouvoir la sécurité de l'information sur l'Internet et à s'attaquer aux problèmes posés par les sites Web inappropriés et illégaux et a mis en place un centre d'opérations pour la sécurité sur l'Internet en vue d'identifier les menaces auxquelles sont exposés les systèmes informatiques et éviter, en coordination avec les autres institutions, que les réseaux informatiques soient utilisés à des fins qui puissent menacer la sécurité nationale. Ce centre d'opérations a également pour objectif de mettre fin aux utilisations illégales des réseaux

informatiques ainsi que de mettre en place un système de surveillance des virus et des courriels indésirables.

4. Par ailleurs, il conviendrait de créer un organe de coordination afin de centraliser les efforts de coopération internationale. Cet organe devrait avoir pour mandat d'élaborer des politiques visant à prévenir et à combattre les utilisations inappropriées des systèmes informatiques et d'adopter des mesures pour parer aux menaces à la sécurité de l'information ainsi que d'élaborer des principes directeurs concernant les mesures de prévention concertées qui pourraient être adoptées.

Examen des concepts internationaux pertinents visant à renforcer la sécurité des systèmes informatiques et télématiques mondiaux

5. Le cybermonde d'aujourd'hui étant interdépendant et transcendant les frontières, il importe de promouvoir le partage des concepts et des principes internationaux visant à promouvoir la sécurité mondiale de l'information car tout problème de sécurité qui surgit dans un pays peut en affecter un autre.

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

6. La communauté internationale pourrait notamment adopter des mesures dans des domaines comme les échanges d'informations, en particulier en ce qui concerne les mesures de prévention et les mesures visant à parer aux menaces à la sécurité de l'information. Il faudrait également resserrer la coopération afin de renforcer et de mettre à niveau les moyens informatiques des différents pays, et les pays développés devraient notamment s'employer à transférer des technologies et des connaissances techniques aux pays les moins avancés pour contribuer à renforcer les capacités de ces derniers. Il faudrait également élaborer des programmes de formation portant sur des questions comme la sensibilisation, la prévention, la détection, la gestion et l'intervention afin de minimiser les risques et les menaces à la sécurité de l'information.

7. Il faut en outre créer un mécanisme de coordination pour relier les activités des différentes institutions concernées et définir les orientations et politiques à suivre afin de faire converger les efforts visant à garantir un certain niveau de sécurité de l'information au plan national.

8. Il y a lieu par ailleurs d'encourager les efforts déployés par certaines institutions internationales, en particulier l'Union internationale des télécommunications (UIT), pour promouvoir la coopération internationale tendant à renforcer la sécurité de l'information. L'UIT a organisé une conférence internationale afin d'échanger des données d'expérience et d'explorer les mesures pouvant être adoptées pour régler les problèmes découlant du mésusage des technologies de l'information. L'UIT a également créé des groupes de travail chargés d'étudier les mesures de nature à renforcer la sécurité de l'information et les gouvernements et les institutions concernées pourront s'inspirer des résultats de leurs travaux et les appliquer.

9. Des équipes d'intervention informatique d'urgence (CERT) devraient également être créées dans chaque pays avec l'assistance des pays ayant acquis une expérience à cet égard.

10. Il importe pour la communauté internationale d'adopter des mesures en vue de protéger les infrastructures critiques nationales contre les cyberattaques et de fournir une coopération ou une assistance rapide dans ce domaine, et il faudrait explorer conjointement les moyens d'éliminer ces risques ou de les réduire au minimum.

11. Enfin, il faudrait encourager l'Organisation des Nations Unies à concentrer davantage son attention sur la question de la sécurité de l'information et l'Organisation pourrait peut-être discuter des règles et règlements qui pourraient être adoptés concernant les moyens de guerre informatique et publier chaque année des rapports sur la vulnérabilité des systèmes informatiques et télématiques et les menaces auxquelles ceux-ci sont exposés.

Ukraine

[Original : russe]
[20 mai 2009]

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

2. La moitié des infractions informatiques enregistrées dans le monde sont liées à l'accès non autorisé à des données électroniques. De plus en plus, ces infractions sont motivées par l'appât du gain et elles sont de plus en plus destructrices. Le nombre d'infractions perpétrées par des gangs transnationaux augmente.

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

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

5. La lutte contre la délinquance liée aux technologies de l'information soulève de nombreux problèmes d'ordre juridique, les preuves électroniques étant immatérielles et souvent éphémères. La coopération internationale est d'autant plus importante que les problèmes liés à la cybercriminalité sont difficiles à résoudre et,

au bout du compte, il importe que tous les États disposent simultanément des moyens juridiques, procéduraux et normatifs nécessaires.

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

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

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

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

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

11. En coopération avec la Police nationale des Pays-Bas et le Service fédéral de sécurité de la Russie, l'Ukraine a mené, vers la fin de 2008, une opération coordonnée de répression des activités illicites d'un gang international de pirates informatiques qui s'attaquait aux ressources financières d'établissements de crédit financiers en accédant illégalement à leurs systèmes automatisés.

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

13. Ainsi, en application de la Convention internationale sur la cybercriminalité, un réseau viable et convivial de centres de liaison nationaux fonctionnant jour et nuit, sept jours sur sept, a été créé, regroupant les pays du G-8 et d'autres États parties à la Convention.

14. Compte tenu de la décision du Président de l'Ukraine portant création d'un tel centre de liaison en Ukraine, un Groupe de travail interdépartemental composé de fonctionnaires du Service de sécurité, du Ministère des affaires intérieures, du Bureau du procureur général et du Ministère de la justice de l'Ukraine élabore des projets de loi sur la ratification de la Convention sur la cybercriminalité, sur la modification de la loi de l'Ukraine concernant la ratification de la Convention sur les télécommunications ainsi que sur la structure et les effectifs du Service de la sécurité de l'Ukraine et sur le Décret présidentiel concernant l'organisation des travaux du centre de liaison.

15. En application du Décret du Président de l'Ukraine, le Service de la sécurité de l'Ukraine fait actuellement le nécessaire pour enregistrer le centre de liaison auprès du réseau international.

16. Grâce aux travaux de ce centre de liaison, les échanges d'informations et la lutte contre la cybercriminalité à l'échelle internationale pourront se faire encore plus efficacement et plus rapidement.

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

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

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

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

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

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

19. Les lois et règlements régissant la protection de l'information en Ukraine sont notamment les suivantes : loi sur les fondements de la sécurité nationale en Ukraine, loi sur l'information, sur la protection de l'information sur les réseaux télématiques, décrets du Président et du Conseil des ministres de l'Ukraine faisant le point de la protection technique de l'information en Ukraine, règlement assurant la protection des données sur les réseaux télématiques, dispositif concernant le raccordement aux réseaux mondiaux de transmission de données et divers textes normatifs déposés auprès du Ministère de la justice applicables aux questions du raccordement des systèmes d'information aux réseaux mondiaux, à la délivrance de licences pour diverses activités, et les dispositions relatives à l'évaluation de la production, s'agissant notamment de la protection de l'information.

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

composantes doivent être conformes aux textes normatifs applicables à la protection de l'information.

21. Pour normaliser les spécifications du Système complexe et des différents systèmes d'information en Ukraine, on a rédigé et mis en application une cinquantaine de textes normatifs à caractère technique définissant les critères d'évaluation du degré de protection des données et permettant de classer les réseaux télématiques de manière à déterminer les modalités d'exécution des travaux concernant la protection des données, ainsi que les critères applicables aux systèmes de protection de l'information et au Système complexe, selon la catégorie de réseau télématique, de la portée et du champ d'application de l'information traitée.

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

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

24. En réponse à de tels actes, la communauté mondiale a constitué un vaste réseau décentralisé de structures d'intervention rapide en cas d'incidents menaçant la sécurité et les ressources informationnelles, à savoir des équipes d'intervention d'urgence en matière de sécurité informatique (CERT). La coordination est assurée au niveau international par l'organisation internationale FIRST, chargée d'intervenir en cas d'urgence.

25. Pour disposer de textes législatifs et réglementaires similaires, l'administration des liaisons spéciales a proclamé le décret n° 94 du 10 juin 2008 confirmant les dispositions concernant la coordination des organes gouvernementaux, des organes des autorités locales, des formations militaires, des entreprises, des établissements et organisations, quel que soit le type de propriété, pour prévenir et identifier les actes illicites visant les ressources informationnelles sur les réseaux télématiques et en éliminer les conséquences.

26. En application du décret susmentionné, on a créé une page Web et une adresse électronique sur Internet (www.cert.gov.ua).

27. Des mesures sont prises en Ukraine, compte tenu de l'expérience internationale en matière de sécurité des ressources informatiques : on a créé, sur la base de la liaison spéciale, une coordination nationale chargée d'assurer la sécurité sur les réseaux télématiques (CERT-UA) qui a été accréditée auprès de FIRST. À cette fin, on a organisé le 17 mars 2009 une rencontre de représentants de l'administration de la liaison gouvernementale spéciale et du Haut conseiller sur les questions de sécurité de l'information auprès de l'organe plénipotentiaire finlandais de réglementation des télécommunications (FICORA).

28. Bien que CERT-UA ne soit pas accréditée auprès de la FIRST, la partie ukrainienne a reçu en 2006-2008 plus de 200 avis des CERT de Finlande,

d'Australie, d'Autriche, de Slovénie et d'autres pays concernant des actes non autorisés perpétrés sur l'Internet par des usagers ukrainiens. En conséquence, plus de 250 courriels ont été adressés aux fournisseurs concernés, en vue de localiser les sources des programmes nocifs et des virus. De plus en mai 2007, des mesures ont été prises pour faire cesser les attaques du type « déni de service distribué » lancées de sources ukrainiennes contre des serveurs estoniens puis, en octobre 2007, une attaque similaire lancée contre le site Web du Président de l'Ukraine a été interrompue.

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

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

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