Nations Unies A/65/201

Assemblée générale

Distr. générale
30 juillet 2010
Français
Original : anglais

Soixante-cinquième session
Point 94 de l'ordre du jour provisoire*
Les progrès de la téléinformatique dans le contexte de la sécurité internationale

Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale

Note du Secrétaire général

Le Secrétaire général a l'honneur de transmettre le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale. Le Groupe d'experts gouvernementaux a été créé en application du paragraphe 4 de la résolution 60/45 de l'Assemblée générale.

* A/65/150.

10-46958 (F) 170810 180810

Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale

Résumé

Les risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information figurent parmi les problèmes les plus graves du XXIe siècle. Ces risques, qui ont des origines très diverses, prennent la forme d'activités perturbatrices qui ciblent les personnes, les entreprises et les infrastructures nationales comme les pays. Ils ont des effets qui peuvent compromettre fortement la sécurité publique, la sécurité des pays et la stabilité de la communauté internationale avec ses interconnexions mondiales.

Les technologies de l'information et des communications (TIC) sont de plus en plus utilisées dans des infrastructures vitales, ce qui crée de nouvelles vulnérabilités et de nouvelles possibilités de perturbations. Les interconnexions entre télécommunications et Internet étant complexes, n'importe quel dispositif informatique peut être la source ou la cible d'une utilisation malveillante de plus en plus élaborée. Bivalentes par nature, les mêmes TIC qui sous-tendent un commerce électronique robuste peuvent également servir à menacer la paix internationale et la sécurité nationale.

Il peut être difficile d'établir l'origine d'un acte perturbateur, l'identité de son auteur ou sa motivation. Souvent, ce n'est qu'à partir de la cible, des conséquences ou d'autres éléments indirects que l'on peut déduire l'identité de l'auteur, qui peut agir depuis pratiquement n'importe quel lieu. Ces particularités facilitent l'utilisation des TIC pour des activités perturbatrices. L'absence de certitude sur l'origine de ces actes, et d'une communauté de vues sur la question, est à l'origine du risque d'instabilité et de confusion.

Il est de plus en plus souvent signalé que des États développent des techniques informatiques comme instruments de guerre et de renseignement, ainsi qu'à des fins politiques. Que des personnes, des groupes ou des organisations, notamment criminelles, agissant pour le compte d'autrui, exécutent des activités perturbatrices en ligne, suscite une inquiétude croissante. La complexité et la portée de plus en plus étendue des activités criminelles accroissent les possibilités d'actes pernicieux. Même si on n'a guère d'indices d'une utilisation des TIC pour des opérations de perturbation à des fins terroristes, cette éventualité pourrait devenir plus réelle à l'avenir.

Seule permettra de faire face aux défis du XXIe siècle la coopération réussie entre partenaires partageant une communauté de vues. Il importe que les États collaborent entre eux et avec le secteur privé et la société civile; une large coopération internationale est indispensable pour que les mesures visant à améliorer la sécurité de l'information soient efficaces. Le rapport du Groupe d'experts gouvernementaux fait des recommandations en vue d'améliorer la concertation entre États, de façon à réduire les risques et à protéger les infrastructures nationales et internationales vitales.

Table des matières

Avant-propos du Secrétaire général

Il y a 10 ans, nous n'aurions pas pu prévoir à quel point les technologies de l'information et des télécommunications seraient intégrées dans notre vie quotidienne ni à quel point nous en deviendrions tributaires. Ces technologies ont créé une communauté internationale aux interconnexions mondiales – dont les avantages sont immenses, mais qui apporte également des vulnérabilités et des risques.

Des progrès considérables ont été réalisés dans la prise en compte des ramifications des nouvelles technologies. Mais la tâche est ardue et nous commençons à peine à élaborer les normes, les lois et les modes de coopération nécessaires dans ce nouvel environnement où passe l'information.

Sachant cela, j'ai nommé un groupe d'experts gouvernementaux de 15 États, le chargeant d'étudier les risques qui se posent ou pourraient se poser à cet égard et de recommander des moyens par lesquels y parer. Je remercie le Président du Groupe et les experts de la diligence et de la rigueur qu'ils ont apportées à leur travail, dont l'aboutissement est le présent rapport, exposé concis du problème et des voies qui s'offrent pour l'avenir.

L'Assemblée générale a un rôle important à jouer en matière de sécurisation des technologies de l'information et des communications, aux niveaux national et international. Il est impératif que les États Membres se concertent pour élaborer des perspectives communes. Il est également crucial qu'ils coopèrent concrètement pour échanger les meilleures pratiques et les informations, pour renforcer les capacités des pays en développement, et pour réduire le risque de confusion, qui pourrait gêner la communauté internationale pour bien gérer un incident grave survenant dans le cyberspace.

C'est là un programme chargé pour la suite des travaux. Le présent rapport servira à lancer la mise en place du cadre international de sécurité et de stabilité que rendent indispensables les nouvelles technologies. J'invite les États Membres et le grand public à se pencher attentivement sur l'analyse et les recommandations qui y sont présentées.

Lettre d'envoi

Le 16 juillet 2010

J'ai l'honneur de présenter ci-après le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale. Le Groupe d'experts gouvernementaux a été créé en 2009 en application du paragraphe 4 de la résolution 60/45 de l'Assemblée générale. En ma qualité de Président du Groupe, j'ai le plaisir de vous faire savoir que le présent rapport a fait l'objet d'un consensus.

Dans cette résolution, intitulée « Les progrès de la téléinformatique dans le contexte de la sécurité internationale », l'Assemblée générale a demandé que soit créé un groupe d'experts gouvernementaux, désignés sur la base d'une répartition géographique équitable, chargé de poursuivre l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information et des mesures de coopération qui pourraient être prises pour y parer, ainsi que l'étude des principes susceptibles de renforcer la sécurité des systèmes mondiaux dans le domaine de la téléinformatique. Elle a demandé au Secrétaire général de lui présenter un rapport sur les résultats de ces travaux à sa soixante-cinquième session.

En application de cette résolution, ont été nommés des experts des 15 pays suivants : Afrique du Sud, Allemagne, Bélarus, Brésil, Chine, Estonie, États-Unis d'Amérique, Fédération de Russie, France, Inde, Israël, Italie, Qatar, République de Corée, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord. La liste des experts figure en annexe au présent rapport.

Le Groupe d'experts gouvernementaux a tenu quatre sessions : la première, du 24 au 26 novembre 2009, à Genève; la deuxième, du 11 au 15 janvier 2010, au Siège de l'ONU; la troisième, du 21 au 25 juin 2010, à Genève; et la quatrième, du 12 au 16 juillet, au Siège de l'ONU.

Le Groupe a procédé à un large échange de vues détaillées sur les progrès de la téléinformatique dans le contexte de la sécurité internationale. Il a tenu compte des vues exprimées par les États Membres suite aux résolutions 60/45, 61/54, 62/17 et 63/37 de l'Assemblée générale intitulées « Les progrès de la téléinformatique dans le contexte de la sécurité internationale », ainsi que des contributions et des documents de référence fournis par ses propres membres.

Le Groupe tient à remercier l'Institut des Nations Unies pour la recherche sur le désarmement, représenté par James Lewis et Kerstin Vignard, du rôle de consultant qu'il a joué auprès de lui. Il tient également à exprimer sa reconnaissance à Ewen Buchanan, fonctionnaire de l'information du Service de l'information et de la sensibilisation au Bureau des affaires de désarmement du Secrétariat, qui a assumé les fonctions de secrétaire du Groupe, ainsi qu'aux autres fonctionnaires du Secrétariat qui lui ont apporté leur concours.

Le Président du Groupe
(*Signé*) Andrey V. **Krutskikh**

I. Introduction

1. Les risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information sont au nombre des problèmes les plus ardus du XXI^{e} siècle. Ils peuvent nuire gravement à l'économie des pays, ainsi qu'à la sécurité nationale et internationale. Ils ont des origines très diverses et prennent la forme d'activités perturbatrices qui ciblent les personnes, les entreprises et les infrastructures nationales comme les pays. Ils ont des effets qui peuvent compromettre gravement la sécurité publique, la sécurité des pays et la stabilité de la communauté internationale avec ses interconnexions mondiales.

2. Les TIC présentent des particularités qui leur sont propres et rendent difficile de parer aux risques que pourraient rencontrer les États et les autres utilisateurs. Les TIC sont omniprésentes et facilement disponibles. Intrinsèquement, elles ne sont ni militaires ni civiles par nature, et sont utilisées à des fins qui dépendent essentiellement des motifs de l'utilisateur. Les réseaux sont souvent contrôlés et exploités par le secteur privé ou par des particuliers. Les interconnexions entre télécommunications et Internet étant complexes, n'importe quel dispositif informatique peut être la source ou la cible d'une utilisation malveillante de plus en plus élaborée. Il est facile d'en dissimuler l'utilisation malveillante. L'origine d'un acte perturbateur, l'identité de son auteur ou sa motivation peuvent être difficiles à établir. Souvent, ce n'est qu'à partir de la cible, des conséquences ou d'autres éléments indirects que l'on peut déduire l'identité de l'auteur. Les auteurs de menaces peuvent agir avec impunité ou presque, à partir de n'importe quel lieu. Ces particularités facilitent l'utilisation des TIC à des fins de perturbation.

3. Étant donné les conséquences pour la sécurité internationale, l'Assemblée générale des Nations Unies a demandé au Secrétaire général, avec l'aide d'experts gouvernementaux, d'examiner les risques qui se posent dans le domaine de la sécurité de l'information ainsi que les principes internationaux pertinents, et de proposer des mesures de coopération qui pourraient renforcer la sécurité des systèmes téléinformatiques mondiaux.

II. Menaces, risques et vulnérabilités

4. Le réseau mondial des TIC est devenu le théâtre d'activités perturbatrices. Les raisons en sont très diverses : simple étalage de promesses techniques, détournement d'argent ou d'informations, ou encore prolongement d'un conflit étatique. À l'origine de ces menaces, on peut trouver des acteurs non étatiques (criminels et, éventuellement, terroristes) mais aussi des États. Les TIC peuvent servir à endommager des ressources électroniques et des infostructures. Bivalentes par nature, les mêmes TIC qui sous-tendent un commerce électronique robuste peuvent également servir à menacer la paix internationale et la sécurité nationale.

5. De nombreux outils ou procédés malveillants sont créés par des criminels ou des pirates informatiques. Les activités criminelles gagnant en complexité et en portée, la possibilité d'actes pernicieux augmente elle aussi.

6. Il y a peu d'indications jusqu'à présent de quelque tentative terroriste visant à corrompre ou désactiver les infostructures ou à exécuter des opérations en se servant de moyens informatiques, mais on pourrait les voir se multiplier à l'avenir. Pour l'heure, les terroristes exploitent surtout ces technologies pour communiquer,

collecter des informations, recruter, organiser, promouvoir leurs idées et leurs activités et demander des fonds, mais ils pourraient à terme y recourir pour un attentat.

7. Il est de plus en plus souvent signalé que des États développent des techniques informatiques comme instruments de guerre et de renseignement, ainsi qu'à des fins politiques. L'absence de certitude sur l'origine de ces actes, et d'une communauté de vues sur ce qui constitue un comportement acceptable pour un État risque de créer instabilité et confusion.

8. Que des personnes, des groupes ou des organisations, notamment criminelles, agissant pour le compte d'autrui, exécutent en ligne des activités perturbatrices suscite une inquiétude croissante. Qu'ils agissent pour des motifs financiers ou autres, ces intermédiaires peuvent offrir toute une gamme de services pernicieux à des acteurs étatiques et non étatiques.

9. L'utilisation croissante des TIC dans des infrastructures vitales crée de nouvelles vulnérabilités et de nouvelles possibilités de perturbations, de même que l'usage de plus en plus répandu de matériel de communication mobile et de services sur le Web.

10. Les États craignent aussi que la chaîne d'approvisionnement des TIC soit influencée ou corrompue d'une façon qui en compromette l'exploitation normale, sûre et fiable. L'incorporation dans les TIC de fonctions malveillantes cachées peut saper la confiance placée dans les produits et les services ainsi que dans le commerce, et nuire à la sécurité nationale.

11. Le niveau de capacité et de sécurité des TIC étant différent selon les États, la vulnérabilité du réseau mondial en est d'autant plus grande. Les disparités entre les législations et les pratiques nationales peuvent également créer des obstacles à la mise en place d'un environnement numérique sûr et robuste.

III. Mesures de coopération

12. Les risques associés aux réseaux à interconnexions mondiales appellent des réactions concertées. Ces 10 dernières années, les États Membres ont réaffirmé à maintes reprises que la coopération internationale était indispensable face aux menaces qui pèsent sur la sécurité informatique, pour la lutte contre l'utilisation malveillante des technologies de l'information, la mise en place d'une culture mondiale de cybersécurité et de la promotion des autres mesures voulues pour réduire les risques.

13. Une action internationale a été engagée ces 10 dernières années contre la menace de la cybercriminalité, notamment à l'Organisation de coopération de Shanghai, à l'Organisation des États américains, à l'Association de coopération économique Asie-Pacifique, au Forum régional de l'Association des nations de l'Asie du Sud-Est (ASEAN), à la Communauté économique des États de l'Afrique de l'Ouest, à l'Union africaine, à l'Union européenne, à l'Organisation pour la sécurité et la coopération en Europe et au Conseil de l'Europe, ainsi qu'entre États, sous la forme d'initiatives bilatérales.

14. Il convient d'accorder l'attention requise aux domaines d'intérêt transnational qui ne sont pas liés à la criminalité, tels que le risque de confusion dû à une divergence de vues sur les normes internationales visant l'utilisation des TIC par les

États, qui pourrait compromettre la gestion de crise en cas d'incident grave. C'est une raison qui devrait porter à élaborer des mesures visant à renforcer la coopération là ou c'est possible, ces mesures pourraient également être conçues de manière à favoriser le partage des meilleures pratiques, aider à gérer les incidents, instaurer la confiance, réduire les risques et accroître la transparence et la stabilité.

15. Plus les activités de perturbation exploitant les TIC deviennent complexes et dangereuses, plus il est clair qu'aucun État ne peut faire face seul à ces menaces. Seule permettra de faire face aux défis du XXI^{e} siècle la coopération réussie entre des partenaires partageant une communauté de vues. Il importe que les États collaborent entre et avec le secteur privé et la société civile; une large coopération internationales est indispensable pour que les mesures visant à améliorer la sécurité de l'information soient efficaces. Il faut donc que la communauté internationale se penche sur la nécessité de mettre en place des activités et des mécanismes de coopération.

16. Les accords existants comprennent des normes qui intéressent l'usage que font les États des TIC. Compte tenu des particularités qui sont propres à ces dernières on pourrait envisager d'élaborer peu à peu des normes supplémentaires.

17. Il est crucial de renforcer les capacités pour garantir la sécurité des TIC au niveau mondial, aider les pays en développement à améliorer la sécurité de leurs infostructures essentielles et combler le fossé qui existe actuellement en matière de sécurité informatique. Il faudra une collaboration internationale étroite pour renforcer les capacités des États qui pourraient avoir besoin d'aide pour améliorer leur sécurité informatique.

IV. Recommandations

18. Conscient des menaces, des risques et des vulnérabilités que présente actuellement et peut présenter à l'avenir la sécurité informatique, le Groupe des experts gouvernementaux juge utile de recommander ci-après des mesures de confiance et d'autres pour réduire le risque de confusion dû à des perturbations informatiques :

i) Poursuivre la concertation entre États sur des normes éventuelles relatives à l'utilisation des TIC par les États, afin de réduire le risque collectif et de protéger les infrastructures nationales et internationales essentielles;

ii) Adopter des mesures de confiance, de stabilité et de réduction des risques qui répondent aux conséquences de l'utilisation des TIC par les États, avec notamment des échanges de vues entre pays sur l'utilisation des TIC dans les conflits;

iii) Échanger des informations sur les législations nationales et les stratégies de sécurité nationales relatives aux technologies de l'information et des communications, ainsi que sur les techniques, les politiques et les meilleures pratiques;

iv) Définir des moyens d'aider les pays moins développés à renforcer leurs capacités;

v) Mettre en évidence les possibilités d'élaborer des modalités et des définitions communes procédant de la résolution 64/25 de l'Assemblée générale.

Annexe

Liste des membres du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale

M. Vladimir N. Gerasimovich
Chef du Département de la sécurité internationale et du contrôle des armes
Ministère des affaires étrangères
Bélarus

M. Aleksandr Ponomarev (troisième session)
Conseiller de la Mission permanente de la République du Bélarus auprès de l'Office des Nations Unies à Genève

M. Alexandre Mariano Feitosa
Commandant
Marine Corps du Brésil, marine brésilienne
Secrétariat chargé des politiques, de la stratégie et des affaires internationales
Ministère de la défense
Brésil

M. Li Song (première et deuxième sessions)
Directeur général adjoint
Département du contrôle des armements et du désarmement
Ministère des affaires étrangères
Chine

M. Kang Yong (troisième et quatrième sessions)
Directeur général adjoint
Département du contrôle des armements et du désarmement
Ministère des affaires étrangères
Chine

M. Linnar Viik
Professeur associé
Collège d'études informatiques
Estonie

M. Aymeric Simon
Relations internationales
Agence nationale de la sécurité des systèmes d'information
Secrétariat général de la défense et de la sécurité nationale
France

M. Gregor Koebel
Chef de la Division du contrôle des armes classiques
Ministère fédéral des affaires étrangères
Allemagne

M. B. J. Srinath
Directeur principal
Équipe indienne d'intervention d'urgence en matière de sécurité informatique
Département des technologies de l'information
Inde

M^me^ Rodica Radian-Gordon
Directrice
Département du contrôle des armements
Ministère des affaires étrangères
Israël

M. Vincenzo Della Corte (première et troisième sessions)
Directeur du Secteur de la sécurité de la communication
Présidence du Conseil des ministres
Italie

M. Walter Mecchia (deuxième et quatrième sessions)
Secteur de la sécurité de la communication
Présidence du Conseil des ministres
Italie

M. Rashid A. Al-Mohannadi (première session)
Commandant de la Compagnie des transmissions de l'armée de terre
Corps des transmissions Amiri
Qatar

M. Saad M. R. Al-Kaabi
Lieutenant-colonel (ingénieur)
Ministère de la défense
Qatar

M. Lew Kwang-chul
Ambassadeur
Ministère des affaires étrangères et du commerce
République de Corée

M. Andrey V. Krutskikh
Directeur adjoint
Département des nouveaux défis et menaces
Ministère des affaires étrangères
Fédération de Russie

M^me^ Palesa Banda (première session)
Directrice adjointe, Gouvernance d'Internet
Département de la Communication
Afrique du Sud

Maj. Gen. Mario Silvino Brazzoli
Officier chargé des technologies de l'information
Département de la défense
Afrique du Sud

M. Gavin Willis
Équipe des relations internationales
Autorité technique nationale pour la sûreté de l'information (CESG)
Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

M^me^ Michele G. Markoff
Conseillère principale pour les politiques
Bureau des cyberaffaires
Département d'État des États-Unis
États-Unis d'Amérique