Nations Unies A/68/98*

Assemblée générale

Distr. générale
24 juin 2013
Français
Original : anglais

Soixante-huitième session
Point 94 de l'ordre du jour provisoire**
Progrès de l'informatique et des télécommunications et 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 ci-joint 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 66/24 de l'Assemblée générale.

* Nouveau tirage pour raisons techniques (30 juillet 2013).
** A/68/150.

13-37167* (F) 060813 070813

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

Résumé

L'informatique et les communications ont radicalement changé la donne sur le plan de la sécurité internationale. Tout en présentant de précieux avantages économiques et sociaux, ces technologies peuvent également être utilisées à des fins incompatibles avec la paix et la sécurité internationales. L'utilisation de l'informatique à des fins criminelles ou dans le cadre d'actions perturbatrices a notablement augmenté ces dernières années. Les utilisations malveillantes pouvant facilement être maquillées, il est souvent difficile d'en déterminer les auteurs, lesquels peuvent agir en toute impunité, créant ainsi un environnement propice à une exploitation de plus en plus sophistiquée de ces technologies.

Les États Membres ont souvent mis en avant la nécessité de coopérer pour lutter contre les menaces résultant d'utilisations malveillantes de la téléinformatique. La coopération internationale est essentielle pour réduire les risques et renforcer la sécurité. Pour progresser dans ce domaine au niveau international, des initiatives en faveur d'un environnement informatique pacifique, sûr, ouvert et coopératif sont indispensables. Les mesures de coopération qui favoriseraient la stabilité et la sécurité comprennent l'application de normes, de règles et principes de comportement responsable de la part des États, les mesures volontaires pour améliorer la transparence, les activités de renforcement de la confiance entre les États et les initiatives de renforcement des capacités. C'est aux États qu'il incombe de prendre de telles mesures, mais la participation du secteur privé et de la société civile contribuerait à améliorer l'efficacité de la coopération.

Conscient de l'ampleur du défi et des menaces réelles ou potentielles qui pèsent sur la sécurité internationale et s'appuyant sur les recommandations formulées par le Groupe d'experts de 2010 dans son rapport (A/65/201), le Groupe d'experts gouvernementaux de 2013 chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale propose dans le présent rapport des recommandations visant à promouvoir la paix et la sécurité dans le cadre de l'utilisation de la téléinformatique par les États.

Dans le présent rapport, le Groupe d'experts estime essentiel d'appliquer les normes qui découlent du droit international en vigueur régissant l'utilisation de la téléinformatique par les États afin de réduire les risques pour la paix, la sécurité et la stabilité internationales. Il recommande en outre de mener une étude approfondie en vue de définir une vision commune de l'application de ces normes au comportement des États et à l'utilisation qu'ils font des technologies de l'informatique et des communications. Compte tenu de la spécificité du domaine informatique, il souligne également que de nouvelles normes pourraient être élaborées au fil du temps.

Dans son rapport, le Groupe d'experts conclut que le droit international et, en particulier, la Charte des Nations Unies sont applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique ouvert, sûr, pacifique et accessible. Il conclut également que les normes et principes internationaux qui procèdent de la souveraineté étatique s'appliquent à l'utilisation de l'outil informatique par les États ainsi qu'à leur compétence territoriale en matière d'infrastructure informatique; en outre ceux-ci doivent s'acquitter de leurs obligations internationales et répondre des actes contraires au droit international qu'ils commettraient. Il recommande la mise en place de mesures volontaires favorisant la confiance et la transparence, ainsi que de mesures de coopération internationale visant à renforcer les capacités en matière de sécurité informatique, en particulier dans les pays en développement. Il estime qu'un dialogue institutionnel suivi sur ces questions, organisé sous les auspices de l'Organisation des Nations Unies et dans d'autres forums, ferait avancer la mise en œuvre de telles mesures. Les États Membres devraient s'intéresser activement à ce rapport et déterminer les moyens qui leur permettraient de mieux élaborer et appliquer ces recommandations.

Table des matières

		Page
	Avant-propos du Secrétaire général	4
	Lettre d'envoi	5
I.	Introduction	6
II.	Renforcer la coopération pour promouvoir un environnement informatique pacifique, sûr, résilient et ouvert	7
III.	Recommandations sur les normes, règles et principes de comportement responsable des États	8
IV.	Recommandations sur les mesures visant à instaurer la confiance et sur l'échange d'informations	9
V.	Recommandations sur les mesures de renforcement des capacités	11
VI.	Conclusion	12
Annexe		13

Avant-propos du Secrétaire général

L'informatique et les communications font partie de notre quotidien. Si tous les pays saluent les avantages extraordinaires que procure l'informatique, il existe également un large consensus pour considérer que l'utilisation malveillante qui en est faite fait peser des menaces sur la paix et la sécurité internationales.

Le présent rapport contient des recommandations formulées par un groupe d'experts gouvernementaux provenant de 15 États visant à lutter contre les menaces réelles ou potentielles que les États, leurs agents ou des acteurs non étatiques font peser sur la paix et la sécurité internationales en utilisant les technologies de l'informatique et des communications. Il s'est appuyé sur les recommandations formulées en 2010 par le précédent groupe d'experts, qui avait notamment fait état de la nécessité de poursuivre les travaux qu'il avait engagés sur les normes et les moyens de renforcer la confiance et les capacités.

Je me félicite de l'importance accordée par ce rapport au rôle central que jouent la Charte des Nations Unies et le droit international ainsi qu'à la nécessité pour les États de s'acquitter de leurs responsabilités. Les recommandations montre4nt la voie à suivre pour que la sécurité informatique s'inscrive dans le droit et les principes internationaux en vigueur régissant les relations internationales et constituant le fondement de la paix et de la sécurité internationales.

Comme le relève le Groupe d'experts, l'Organisation des Nations Unies joue un rôle important dans la promotion du dialogue entre les États Membres en ce qui concerne la question de la sécurité dans l'utilisation des ressources informatiques par les États et dans le renforcement de la coopération internationale dans ce domaine.

Je remercie la Présidente du Groupe et les experts du soin qu'ils ont apporté à leurs travaux. Le présent rapport constitue la base des efforts qui devront être faits pour renforcer la sécurité et la stabilité dans ce domaine. Je transmets à l'Assemblée générale les recommandations formulées dans le présent rapport, qui constituent un pas décisif dans le cadre des efforts faits au niveau mondial pour réduire les risques liés à l'informatique et aux communications tout en tirant le meilleur parti de ces technologies.

Lettre d'envoi

Le 7 juin 2013

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 a été créé en 2012 en application du paragraphe 4 de la résolution 66/24 de l'Assemblée générale. En ma qualité de Présidente du Groupe, j'ai le plaisir de vous faire savoir que le présent rapport a fait l'objet d'un consensus.

Dans sa résolution 66/24, 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, y compris des normes, des règles et des principes de comportement responsable des États et des mesures de confiance concernant les systèmes informatiques, ainsi que l'étude des principes susceptibles de renforcer la sécurité des systèmes informatiques mondiaux. Elle a demandé au Groupe de tenir compte des évaluations et des recommandations figurant dans le rapport du groupe précédent (A/65/201) et au Secrétaire général de lui présenter un rapport sur les résultats de ces travaux à sa soixante-huitième session.

En application de cette résolution, des experts des 15 pays ci-après ont été nommés : Argentine, Allemagne, Australie, Bélarus, Canada, Chine, Égypte, Estonie, États-Unis d'Amérique, Fédération de Russie, France, Inde, Indonésie, Japon et Royaume-Uni de Grande-Bretagne et d'Irlande du Nord. La liste des experts figure en annexe au présent rapport.

Le Groupe d'experts 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 trois sessions : la première, du 6 au 10 août 2012, au Siège de l'ONU; la deuxième, du 14 au 18 janvier 2013, à Genève; et la troisième, du 3 au 7 juin, au Siège de l'ONU.

Le Groupe tient à remercier pour leurs contributions l'Institut des Nations Unies pour la recherche sur le désarmement, représenté par James Lewis et Kerstin Vignard (deuxième et troisième sessions) et par Ben Baseley-Walker (première session), en tant que consultant. Il tient également à exprimer sa reconnaissance à Ewen Buchanan, du 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.

La Présidente du Groupe
(*Signé*) Deborah **Stokes**

I. Introduction

1. L'avènement de la téléinformatique a obligé à redéfinir la question de la sécurité internationale. Tout en présentant de précieux avantages économiques et sociaux, ces technologies peuvent également être utilisées à des fins incompatibles avec la paix et la sécurité internationales. Au cours des dernières années, l'utilisation des technologies informatiques à des fins criminelles ou dans le cadre d'actions perturbatrices a notablement augmenté.

2. La coopération internationale est essentielle pour réduire les risques et renforcer la sécurité. C'est la raison pour laquelle, dans sa résolution 66/24, l'Assemblée générale a prié le Secrétaire général de poursuivre, avec l'assistance d'un groupe d'experts gouvernementaux, l'examen des risques qui se posent ou pourraient se poser et de lui présenter un rapport sur les résultats de ces travaux à sa soixante-huitième session. Le présent rapport s'appuie sur celui de 2010 (A/65/201), établi par un précédent groupe d'experts, qui a examiné la question et formulé des recommandations pour les travaux à venir.

3. Dans le rapport de 2010, le Groupe d'experts a recommandé de poursuivre la concertation entre États sur des normes relatives à l'utilisation de l'informatique et des communications par les États, afin de réduire le risque collectif et de protéger les infrastructures nationales et internationales essentielles. Il a recommandé l'adoption de mesures de confiance, de stabilité et de réduction des risques qui répondent aux conséquences de l'utilisation de l'informatique et des communications par les États, avec notamment des échanges de vues entre pays sur l'utilisation de la télématique dans les conflits, et un échange d'informations sur les législations nationales et les stratégies, les politiques, les technologies et les meilleures pratiques relatives à la sécurité des systèmes informatiques. Il a souligné la nécessité de renforcer les capacités des États susceptibles d'avoir besoin d'aide pour assurer la sécurité de leurs systèmes informatiques et a proposé que des travaux supplémentaires soient menés pour élaborer des modalités et des définitions communes.

4. Depuis 2010, de nombreuses initiatives bilatérales, régionales et multilatérales qui montrent l'importance croissante accordée au renforcement de la sécurité des systèmes informatiques et de l'utilisation qui en est faite ont été lancées pour réduire les risques qui menacent la sécurité publique et améliorer la sécurité des pays et la stabilité à l'échelle mondiale. Il est dans l'intérêt de tous les États de promouvoir l'utilisation de l'informatique et des communications à des fins pacifiques et de prévenir les conflits qu'elle peut engendrer. Une vision commune des normes, règles et principes qui régissent l'utilisation de la téléinformatique et des mesures de confiance volontaires peuvent jouer un rôle important pour renforcer la paix et la sécurité. Bien que les travaux engagés par la communauté internationale pour relever ces défis n'en soient qu'à leurs prémices, un certain nombre de mesures, de règles et de principes favorisant le comportement responsable des États peuvent être recensés et pris en compte.

Menaces, risques et vulnérabilités

5. L'informatique et les communications peuvent être utilisées à des fins aussi bien légitimes que malveillantes. Tout système informatique peut être la source ou la cible d'abus. Les utilisations malveillantes pouvant être facilement maquillées, il

peut s'avérer difficile d'en déterminer les auteurs, leur permettant ainsi de faire une utilisation de plus en plus sophistiquée de l'outil informatique et d'agir en toute impunité. La connexité mondiale des réseaux informatiques exacerbe ce phénomène. La combinaison de la connexité mondiale, des failles technologiques et des possibilités d'agir de façon anonyme facilite l'utilisation de l'informatique et des communications à des fins déstabilisatrices.

6. Les menaces qui pèsent sur les particuliers, les entreprises, les infrastructures nationales et les gouvernements sont devenues plus pressantes, et les conséquences des actes de malveillance, plus graves. Ces menaces proviennent aussi bien d'acteurs étatiques que non étatiques. En outre, tant des particuliers que des groupes ou des organisations, y compris des organisations criminelles, peuvent se livrer à des activités informatiques malveillantes pour le compte d'États. Les possibilités de mise au point et de diffusion de techniques et d'outils malveillants sophistiqués, tels que les *botnets*, par les États ou des acteurs non étatiques peuvent encore augmenter le risque d'imputer à tort des actes de malveillance ainsi que d'escalade non délibérée. L'absence de vision commune sur ce que devrait être le comportement des États en matière d'utilisation de l'informatique et des communications aggrave les risques pour la paix et la sécurité internationales.

7. Des organisations terroristes utilisent l'informatique et les communications pour communiquer, réunir des informations, recruter des membres, organiser, planifier et coordonner des attaques, promouvoir leurs idées et leurs activités et solliciter des fonds. Si elles se procuraient des logiciels malveillants, elles pourraient les utiliser à des fins de déstabilisation.

8. Les États craignent que l'incorporation aux systèmes informatiques de fonctionnalités malveillantes cachées nuise à leur utilisation sûre et fiable, dérègle la chaîne logistique informatique d'approvisionnement en produits et services, érode la confiance nécessaire aux échanges commerciaux et porte atteinte à la sécurité nationale.

9. Le recours de plus en plus généralisé à l'informatique pour gérer les infrastructures essentielles et les systèmes de contrôle industriels crée de nouvelles possibilités de déstabilisation. L'utilisation croissante de matériel de communication portable, du Web, de réseaux sociaux et de services informatiques en nuage augmente les risques pour la sécurité.

10. Les différences d'un État à l'autre en termes de capacités à assurer la sécurité informatique peuvent aggraver la vulnérabilité d'un monde interconnecté. Les acteurs malveillants utilisent les réseaux informatiques, où qu'ils se trouvent. La disparité des législations, des réglementations et des pratiques nationales relatives à l'utilisation des systèmes informatiques amplifie encore ces vulnérabilités.

II. Renforcer la coopération pour promouvoir un environnement informatique pacifique, sûr, résilient et ouvert

11. Les États Membres ont affirmé à plusieurs reprises la nécessité d'une action concertée contre les menaces que pose l'utilisation malveillante des outils informatiques. Le renforcement de la coopération au niveau international nécessite d'engager plusieurs actions pour promouvoir un environnement informatique

pacifique, sûr, ouvert et coopératif. L'adoption de mesures de coopération susceptibles de favoriser la paix, la stabilité et la sécurité internationales devrait être envisagée, notamment une approche commune du droit international applicable en la matière et des normes, règles et principes de comportement responsable des États qui en découlent.

12. S'il revient aux États de prendre l'initiative pour mener à bien cette tâche, la participation appropriée du secteur privé et de la société civile est à même de rendre la coopération plus efficace.

13. L'Organisation des Nations Unies a un rôle moteur à jouer dans la promotion du dialogue entre les États Membres pour aboutir à une compréhension commune des questions de sécurité informatique, encourager les efforts régionaux, favoriser les mesures de confiance et de transparence et soutenir le renforcement des capacités et la diffusion des meilleures pratiques.

14. Outre les actions entreprises au sein du système des Nations Unies, d'excellentes initiatives ont été engagées par des organisations internationales et des entités régionales telles que l'Union africaine, le Forum régional de l'Association des nations de l'Asie du Sud-Est (ASEAN), l'Association de coopération économique Asie-Pacifique, le Conseil de l'Europe, la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), l'Union européenne, la Ligue des États arabes, l'Organisation des États américains (OEA), l'Organisation pour la sécurité et la coopération en Europe (OSCE) et l'Organisation de Shanghai pour la coopération. Ces initiatives devront être prises en compte dans les travaux à venir sur la sécurité informatique.

15. Conscient de l'ampleur de la tâche, ainsi que des menaces, des risques et des faiblesses susceptibles de l'entraver, et s'appuyant sur les constatations et les recommandations figurant dans le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale présenté en juillet 2010 (A/65/201), le Groupe d'experts recommande les mesures ci-après.

III. Recommandations sur les normes, règles et principes de comportement responsable des États

16. Afin de réduire les risques pesant sur la paix, la sécurité et la stabilité internationales, il est indispensable que les États appliquent les normes découlant du droit international en vigueur aux questions informatiques. Un examen plus approfondi est nécessaire pour s'entendre sur la façon dont ces normes s'appliqueront au comportement des États et à l'utilisation qu'ils feront des outils informatiques. Compte tenu des caractéristiques propres à ces outils, de nouvelles normes pourraient être progressivement élaborées.

17. Le Groupe d'experts a examiné les opinions et les observations des États Membres sur les progrès de la téléinformatique dans le contexte de la sécurité internationale communiquées en réponse à la demande que leur a faite l'Assemblée générale dans ses résolutions 64/25, 65/41et 66/24, ainsi que les autres mesures figurant dans les résolutions 55/63, 56/121, 57/239, 58/199 et 64/211.

18. Il a pris note du projet de code de conduite international pour la sécurité de l'information (A/66/359) que le Secrétaire général a fait distribuer à la demande des Représentants permanents de la Chine, de l'Ouzbékistan, de la Fédération de Russie et du Tadjikistan, auxquels se sont joints par la suite les Représentants permanents du Kazakhstan et du Kirghizistan.

19. Le droit international et, en particulier, la Charte des Nations Unies sont applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique ouvert, sûr, pacifique et accessible.

20. La politique des États en matière informatique et leur compétence territoriale pour ce qui est des infrastructures informatiques présentes sur leur territoire relèvent de la souveraineté des États et des normes et principes internationaux qui en découlent.

21. Les actions entreprises par les États pour assurer la sécurité informatique doivent se faire dans le respect des droits de l'homme et des libertés fondamentales énoncés dans la Déclaration universelle des droits de l'homme et dans les autres instruments internationaux.

22. Les États doivent intensifier leur coopération afin de lutter contre l'utilisation des outils informatiques à des fins criminelles ou terroristes, harmoniser leurs procédures juridiques si nécessaire et renforcer concrètement la collaboration entre leurs services de police et leurs ministères publics respectifs.

23. Les États sont tenus d'honorer leurs obligations internationales quant aux faits internationalement illicites qui leur sont imputables. Ils s'interdisent d'utiliser leurs agents pour commettre de tels actes et veillent à ce que des agents non étatiques n'utilisent pas leur territoire pour faire un usage illégal des outils informatiques.

24. Les États doivent encourager le secteur privé et la société civile à jouer un rôle approprié dans le renforcement de la sécurité informatique, notamment en ce qui concerne la chaîne logistique des produits et services informatiques.

25. Les États Membres devraient réfléchir à la meilleure façon de coopérer dans l'application des normes et des principes de comportement responsable susmentionnés, tout en s'intéressant au rôle que le secteur privé et les organisations de la société civile pourraient y jouer. Ces normes et ces principes confortent l'action de l'Organisation des Nations Unies et des groupes régionaux et servent de base aux travaux qui devront être entrepris pour instaurer la confiance.

IV. Recommandations sur les mesures visant à instaurer la confiance et sur l'échange d'informations

26. Des mesures facultatives peuvent être mises en place pour promouvoir la confiance entre les États et contribuer à réduire les risques de conflit en améliorant la prévisibilité et en limitant les malentendus. Elles peuvent permettre d'atténuer notablement les préoccupations concernant l'utilisation que font les États des outils informatiques et de progresser de manière significative vers une plus grande sécurité internationale. Les États devraient envisager d'élaborer des mesures de confiance susceptibles d'améliorer la transparence, la prévisibilité et la coopération, notamment :

a) L'échange de vues et d'informations, à titre facultatif, sur les stratégies et les politiques nationales, les meilleures pratiques, les processus de prise de décisions, les organisations nationales compétentes et les mesures visant à améliorer la coopération internationale. Il reviendra aux États de déterminer l'ampleur des informations qu'ils voudront bien transmettre. Celles-ci pourront être partagées au niveau bilatéral, au sein de groupes régionaux ou au sein d'autres instances internationales;

b) La mise en place de structures de concertation bilatérale, régionale ou multilatérale pour renforcer la confiance, où pourront être organisés des ateliers, des séminaires et des exercices destinés à approfondir les réflexions menées au niveau national sur la façon de prévenir les incidents résultant de l'utilisation par les États des outils informatiques et sur les moyens de gérer ces incidents en fonction de leur évolution;

c) Le partage accru entre les États d'informations sur les incidents de sécurité informatique, par le biais d'une utilisation plus efficace des canaux de communication disponibles ou par la mise en place de nouveaux canaux et mécanismes adéquats pour recevoir, rassembler, analyser et partager les informations sur ces incidents, en vue de leur apporter une réponse immédiate, les résoudre et atténuer leurs effets. Les États devront prévoir de se communiquer les informations relatives à leurs points de contact nationaux, afin de développer et d'améliorer les canaux de communication actuels pour la gestion des crises, et favoriser la création de dispositifs d'alerte rapide;

d) L'échange d'informations et le dialogue entre les équipes d'intervention informatique d'urgence nationales, à un niveau bilatéral, au sein de groupes formés par de telles équipes ou au sein d'autres instances, afin de promouvoir les échanges aux niveaux politique et stratégique;

e) L'intensification de la coopération pour parer aux incidents susceptibles d'endommager les outils informatiques ou les grandes infrastructures tributaires de systèmes informatiques de contrôle industriel. Les États pourront notamment définir des règles de conduite et les meilleures pratiques pour faire face aux actes déstabilisateurs perpétrés par des agents non étatiques;

f) L'amélioration des dispositifs de coopération judiciaire et policière afin de réduire les incidents susceptibles d'être interprétés à tort comme des actes d'hostilité de la part d'un État permettrait de renforcer la sécurité internationale.

27. Ces premières mesures de confiance permettront d'acquérir une expérience pratique et d'orienter utilement les travaux ultérieurs. Il revient aux États d'encourager les initiatives prises aux niveaux bilatéral et multilatéral, et de s'en inspirer, notamment de celles menées au sein de groupes régionaux comme l'Union africaine, le Forum régional de l'ASEAN, l'Union européenne, la Ligue des États arabes, l'OEA, l'OSCE et l'Organisation de Shanghai pour la coopération. Les États s'appuieront sur ces travaux pour promouvoir l'adoption de mesures complémentaires et faciliter la diffusion des meilleures pratiques, compte tenu des différences entre les nations et les régions.

28. S'il revient aux États de prendre l'initiative pour élaborer des mesures de confiance, la participation appropriée du secteur privé et de la société civile est à même d'améliorer la qualité de leurs travaux.

29. Compte tenu de la vitesse à laquelle se développent les outils informatiques ainsi que de l'ampleur de la menace, le Groupe d'experts estime qu'il est indispensable d'aboutir à une définition commune du comportement responsable des États en matière informatique et de renforcer concrètement la coopération. Pour ce faire, il recommande l'instauration d'un dialogue institutionnel régulier sous l'égide de l'Organisation des Nations Unies, aussi large que possible, ainsi que la mise en place d'un dialogue régulier au sein des instances bilatérales, régionales et multilatérales et des autres organisations internationales.

V. Recommandations sur les mesures de renforcement des capacités

30. Le renforcement des capacités est essentiel à la mise en œuvre à l'échelle mondiale d'une action efficace de collaboration pour assurer la sécurité informatique. Certains États pourront avoir besoin d'aide pour améliorer la sécurité de leurs grandes infrastructures informatiques, renforcer leurs compétences techniques et mettre en place une législation, des stratégies et des cadres réglementaires adaptés afin de respecter leurs engagements, ainsi que pour combler les lacunes de leurs systèmes informatiques.

31. À cet égard, les États travaillant en collaboration avec les organisations internationales, dont les organismes des Nations Unies, et le secteur privé doivent déterminer les meilleurs moyens de fournir une aide technique ou autre aux pays ayant besoin de renforcer leurs capacités en matière de sécurité informatique, notamment aux pays en développement.

32. En se fondant sur les résolutions et les rapports précédents de l'Organisation des Nations Unies sur le renforcement des capacités, notamment la résolution 64/211 de l'Assemblée générale, les États sont invités à prendre les mesures ci-après :

a) Soutenir, aux niveaux bilatéral, régional, multilatéral et international, les actions de renforcement des capacités pour assurer la sécurité des outils et des infrastructures informatiques, renforcer les cadres juridiques, les moyens policiers et judiciaires et les stratégies au niveau national, combattre l'utilisation des outils informatiques à des fins criminelles ou terroristes et encourager la recherche et la diffusion des meilleures pratiques;

b) Créer et renforcer les capacités d'intervention en cas d'incident, notamment les équipes d'intervention informatique d'urgence, et améliorer la coopération entre ces équipes;

c) Soutenir la mise en place d'initiatives de formation, d'apprentissage en ligne et d'information dans le domaine de la sécurité informatique, de façon à réduire la fracture numérique et aider les pays en développement à se tenir informés des changements de politique internationale en la matière;

d) Intensifier la coopération, le partage des connaissances et le transfert de technologies en matière de gestion des incidents informatiques, à destination notamment des pays en développement;

e) Encourager les instituts de recherche et les universités à conduire de nouveaux travaux et de nouvelles études sur les questions de sécurité informatique. Les États devraient également se pencher sur le rôle que pourraient jouer dans ce

domaine les instituts de recherche et de formation de l'Organisation des Nations Unies, qui ont pour mandat de soutenir les États Membres de l'Organisation et la communauté internationale.

33. Le Groupe d'experts souligne enfin que les progrès réalisés en matière de sécurité informatique, par le biais notamment du renforcement des capacités, pourraient également contribuer à la réalisation de l'objectif 8 des objectifs du Millénaire pour le développement, lequel prévoit de « mettre en place un partenariat mondial pour le développement ».

VI. Conclusion

34. En matière de sécurité internationale dans l'utilisation que font les États des outils informatiques, les progrès se feront par étapes, chacune d'elles préparant la suivante. Cette démarche itérative est rendue nécessaire compte tenu de l'évolution constante du cadre technologique et de l'augmentation régulière du nombre d'utilisateurs informatiques. Les recommandations figurant dans le présent rapport découlent de travaux précédents : leur mise en œuvre et leurs améliorations successives permettront de renforcer la confiance entre toutes les parties prenantes. Le Groupe d'experts recommande aux États d'accorder une attention particulière au présent rapport et d'examiner comment ces recommandations peuvent être appliquées et approfondies.

Annexe

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

Allemagne

Detlev Wolter
Chef de la Direction du contrôle des armements conventionnels et des mesures de confiance et de sécurité, Ministère des affaires étrangères, Berlin

Argentine

Ambassadeur Alfredo Morelli
Coordonnateur du Service de l'énergie et des technologies, Ministère des affaires étrangères et des cultes, Buenos Aires

Australie

Deborah Stokes
Première Secrétaire adjointe au Ministère des affaires étrangères et du commerce extérieur, Canberra

Bélarus

Vladimir N. Gerasimovich
Chef du Département de la sécurité internationale et du contrôle des armements, Ministère des affaires étrangères, Minsk

Canada

Michael Walma
Directeur de la Division de la planification des politiques, Ministère des affaires étrangères et du commerce, Ottawa

Chine

Lei Wang (première et deuxième sessions)
Directeur du Département du contrôle des armements et du désarmement, Ministère des affaires étrangères, Beijing

Zhihua Dong (troisième session)
Conseillère au Département du contrôle des armements et du désarmement, Ministère des affaires étrangères, Beijing

Égypte

Sherif Hashem
Conseiller principal pour la cybersécurité auprès du Ministre des communications et des technologies de l'information, Ministère des communications et des technologies de l'information, Le Caire

Estonie

Linnar Viik
Directeur par intérim du Collège estonien des technologies de l'information, Tallinn

États-Unis d'Amérique

Michele G. Markoff
Coordonnatrice adjointe des questions cyber et Internet, Bureau du Secrétaire d'État, Département d'État, Washington

Fédération de Russie

Andrey V. Krutskikh
Coordonnateur spécial pour les affaires politiques et l'utilisation des outils informatiques, Ambassadeur itinérant, Ministère des affaires étrangères, Moscou

France

Jean-François Blarel
Secrétaire général adjoint et Coordonnateur des questions cyber et Internet, Ministère des affaires étrangères, Paris

Inde

Harsh K. Jain
Vice-Secrétaire et Chef de la Division de la gouvernance en ligne et des technologies de l'information, Ministère des affaires étrangères, New Delhi

Indonésie

Febrian A. Ruddyard (première session)
Directeur en charge de la sécurité internationale et du désarmement, Ministère des affaires étrangères, Jakarta

Andy Rachmianto (troisième session)
Ministre-Conseiller de la Mission permanente de l'Indonésie auprès de l'Organisation des Nations Unies, New York

Japon

Ambassadeur Tamotsu Shinotsuka (première session)
Coopération internationale dans le cadre de la lutte contre le terrorisme et la criminalité internationale organisée ainsi que des questions de cyberpolitique, Ministère des affaires étrangères, Tokyo

Ambassadeur Osamu Imai (deuxième et troisième sessions)
Coopération internationale dans le cadre de la lutte contre le terrorisme et la criminalité internationale organisée ainsi que des questions de cyberpolitique, Ministère des affaires étrangères, Tokyo

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

Nicholas Haycock
Directeur adjoint pour les questions de sécurité internationale, Bureau de la cybersécurité et de la protection des informations, Cabinet du Premier Ministre, Londres