Nations Unies A/70/174

Assemblée générale

Distr. générale
22 juillet 2015
Français
Original : anglais

Soixante-dixième session
Point 93 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 l'informatique et des télécommunications dans le contexte de la sécurité internationale

Note du Secrétaire général

Le Secrétaire général a l'honneur de communiquer ci-joint le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Le Groupe a été créé par l'Assemblée générale au paragraphe 4 de la résolution 68/243.

* A/70/150.

15-12404 (F) 200815 200815

Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale

Résumé

Les technologies de l'information et des communications (TIC) ouvrent des possibilités immenses et continuent à gagner en importance pour la communauté internationale. Il existe toutefois des tendances préoccupantes qui présentent des risques pour la paix et la sécurité internationales. Une coopération efficace entre les États est indispensable pour réduire ces risques.

Le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale en 2015 a étudié les risques réels ou potentiels qui résultent de l'utilisation des technologies de l'information et des communications par les États et a réfléchi aux dispositions qui permettraient d'y parer, y compris les normes, les règles, les principes et les mesures de confiance. Il s'est également penché sur l'applicabilité du droit international à l'utilisation de ces technologies par les États. Tout en s'appuyant sur les travaux des précédents groupes, le groupe actuel a réalisé d'importants progrès sur ces questions.

Le présent rapport approfondit nettement l'étude des normes. Le Groupe a recommandé que les États coopèrent en vue de prévenir les pratiques informatiques nocives et ne permettent pas sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications. Il a préconisé un renforcement des échanges d'informations et de l'assistance mutuelle pour les poursuites pénales engagées en cas d'utilisation terroriste ou criminelle de ces technologies. Le Groupe a souligné que, dans le cadre de ces activités, les États devraient garantir le plein respect des droits de l'homme, y compris le droit à la vie privée et la liberté d'expression.

L'une des recommandations importantes était qu'un État ne devrait pas mener ou soutenir sciemment une activité informatique qui endommage intentionnellement une infrastructure essentielle ou compromet l'utilisation et le fonctionnement d'une telle infrastructure. Les États devraient aussi prendre les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux TIC. Ils ne devraient pas porter atteinte aux systèmes d'information des équipes d'intervention d'urgence agréées d'un autre État ni se servir de telles équipes pour se livrer à des activités internationales malveillantes. Les États devraient encourager le signalement responsable des failles informatiques, prendre des mesures raisonnables pour garantir l'intégrité de la chaîne logistique et prévenir la prolifération des techniques et des outils informatiques malveillants, ainsi que des fonctionnalités cachées malveillantes.

Les mesures de confiance permettent d'accroître la coopération et la transparence et de réduire le risque de conflit. Le Groupe a recensé plusieurs mesures de confiance volontaires qui contribueraient à accroître la transparence et a proposé que les États en envisagent d'autres pour renforcer la coopération. Il a appelé à un dialogue régulier à large participation sous les auspices de l'Organisation des

Nations Unies ainsi que par le biais d'instances bilatérales, régionales ou multilatérales. Les États sont responsables au premier chef du maintien d'un environnement informatique sûr et pacifique, mais la participation appropriée du secteur privé, du monde universitaire et de la société civile améliorerait la coopération internationale.

Le renforcement des capacités est indispensable à la coopération et au renforcement de la confiance. Le rapport publié en 2013 par le Groupe constitué à cette époque (document A/68/98) appelait la communauté internationale à apporter son concours à l'amélioration de la sécurité des infrastructures informatiques essentielles et au renforcement des compétences techniques et à donner des conseils sur la législation, les stratégies et la réglementation adaptées. Le Groupe actuel a repris ces conclusions et a souligné que tous les États peuvent apprendre les uns des autres sur les risques et sur les moyens efficaces d'y parer.

Le Groupe a insisté sur l'importance du droit international, de la Charte des Nations Unies et du principe de souveraineté comme fondements d'une meilleure sécurité dans l'utilisation des TIC par les États. Tout en convenant de la nécessité d'approfondir la question, le Groupe a noté que les États avaient implicitement le droit de prendre des mesures conformes au droit international et reconnues par la Charte. Il a également rappelé les principes de droit international reconnus, y compris, lorsqu'ils sont applicables, les principes d'humanité, de nécessité, de proportionnalité et de discrimination.

Dans le cadre de ses réflexions pour de futurs travaux, le Groupe a proposé que l'Assemblée générale envisage de créer un nouveau groupe d'experts gouvernementaux en 2016.

Le Groupe demande aux États Membres d'examiner activement ses recommandations et d'étudier comment celles-ci pourraient être précisées et mises en œuvre à l'avenir.

Table des matières

Avant-propos du Secrétaire général

Peu de technologies ont aussi puissamment contribué à transformer les économies, les sociétés et les relations internationales que les technologies de l'information et des communications (TIC) : le cyberespace touche tous les aspects de notre vie. Les bénéfices sont considérables, mais il existe aussi des risques. Seule la coopération internationale permettra de rendre le cyberespace stable et cette coopération doit reposer sur le droit international et sur les principes de la Charte des Nations Unies.

Le présent rapport contient des recommandations formulées par des experts gouvernementaux de 20 États différents en vue de parer aux risques réels ou naissants que des États et des acteurs non étatiques font peser sur la paix et la sécurité internationale en utilisant les technologies de l'information et des communications. Ces experts se sont appuyés sur des rapports de consensus publiés en 2010 et en 2013 et proposent des idées sur les normes à élaborer, les mesures de confiance et de renforcement des capacités et l'application du droit international.

L'un des problèmes complexes qui est apparu est l'utilisation malveillante croissante de ces technologies par des extrémistes, des terroristes et des groupes criminels organisés. Le présent rapport contient des propositions qui peuvent favoriser la lutte contre cette tendance préoccupante et contribuer à la formulation de mon plan d'action pour la prévention de l'extrémisme violent, qui sera présenté prochainement.

Tous les États ont intérêt à rendre le cyberespace plus sûr. Nos efforts dans ce domaine doivent soutenir l'engagement mondial à promouvoir un Internet ouvert, sûr et pacifique. Dans cet esprit, je recommande ce rapport à l'attention de l'Assemblée générale et d'un large public international, car il constitue une contribution déterminante pour protéger l'environnement informatique.

Lettre d'envoi

26 juin 2015

J'ai l'honneur de vous faire tenir ci-joint le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Le Groupe d'experts a été créé en 2014 en application du paragraphe 4 de la résolution 68/243 de l'Assemblée générale sur les progrès de l'informatique et des télécommunications et la sécurité internationale. 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 sa résolution, l'Assemblée générale a demandé que soit constitué en 2014 un groupe d'experts gouvernementaux désignés selon le principe 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 informatique et des mesures collectives qui pourraient être prises pour y parer, y compris les normes, règles ou principes de comportement responsable des États et les mesures de confiance, l'examen des questions de l'utilisation des technologies de l'information et des communications (TIC) dans les conflits et de l'applicabilité du droit international à l'utilisation de ces technologies par les États ainsi que l'étude des principes devant permettre de renforcer la sécurité des systèmes informatiques et télématiques mondiaux, en vue de promouvoir l'adoption de vues communes. Elle a également demandé au Groupe de tenir compte des constatations et recommandations figurant dans le rapport du groupe précédent (document A/68/98) et a prié le Secrétaire général de lui présenter un rapport sur les résultats de ces travaux à sa soixante-dixième session.

En application de cette résolution, des experts des 20 pays suivants ont été nommés : Allemagne, Bélarus, Brésil, Chine, Colombie, Égypte, Espagne, Estonie, États-Unis d'Amérique, Fédération de Russie, France, Ghana, Israël, Japon, Kenya, Malaisie, Mexique, Pakistan, République de Corée et Royaume-Uni de Grande-Bretagne et d'Irlande du Nord. La liste des experts figure en annexe au présent rapport.

Le Groupe a procédé à un large échange de vues détaillées sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Il a tenu quatre sessions : la première, du 21 au 25 juillet 2014, au Siège de l'ONU; la deuxième, du 12 au 16 janvier 2015, à Genève; la troisième, du 13 au 17 avril 2015, comme la quatrième, du 22 au 26 juin 2015, au Siège de l'ONU.

Le Groupe souhaite exprimer sa reconnaissance aux experts qui ont animé les discussions sur le projet de rapport : Ricardo Mor (Espagne), Florence Mangin (France), Katherine Getao (Kenya), Ausaf Ali (Pakistan) et Olivia Preston (Royaume-Uni).

Il tient aussi à remercier l'Institut des Nations Unies pour la recherche sur le désarmement, représenté par James Lewis et Kerstin Vignard, pour le rôle de conseil qu'il joué et à exprimer sa reconnaissance à Ewen Buchanan, du Bureau des affaires de désarmement, 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*) Carlos Luís Dantas Coutinho **Perez**

I. Introduction

1. En application de la résolution 68/243 de l'Assemblée générale sur les progrès de l'informatique et des télécommunications et la sécurité internationale, le Secrétaire général a constitué un groupe d'experts gouvernementaux désignés selon le principe 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 informatique et des mesures collectives qui pourraient être prises pour y parer, y compris les normes, règles ou principes de comportement responsable des États et les mesures de confiance, l'examen des questions de l'utilisation des technologies de l'information et des communications dans les conflits et de l'applicabilité du droit international à l'utilisation de ces technologies par les États ainsi que l'étude des principes devant permettre de renforcer la sécurité des systèmes informatiques et télématiques mondiaux, en vue de promouvoir l'adoption de vues communes.

2. Un environnement informatique ouvert, sûr, stable et accessible est essentiel pour tous et nécessite une coopération efficace entre les États afin de réduire les risques pour la paix et la sécurité internationales. Le présent rapport rend compte des recommandations du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et s'appuie sur les travaux des précédents groupes d'experts (documents A/65/201 et A/68/98). Le Groupe a étudié les principes internationaux et les mesures collectives envisageables qui intéressent son mandat. Il a réaffirmé qu'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 que cette utilisation peut engendrer.

II. Risques réels ou naissants

3. Les TIC ouvrent des possibilités immenses pour le développement économique et social et continuent à gagner en importance pour la communauté internationale. L'environnement informatique mondial présente toutefois des tendances préoccupantes, notamment la hausse spectaculaire du nombre d'actes de malveillance dans lesquels des États ou des acteurs non étatiques sont impliqués. Ces tendances font courir un risque à tous les États et l'utilisation malveillante des TIC peut compromettre la paix et la sécurité internationales.

4. Plusieurs États développent des capacités dans ce domaine à des fins militaires. La probabilité que les TIC soient utilisées dans des conflits futurs entre États augmente.

5. Les attaques les plus graves qui sont menées à l'aide des TIC comprennent celles qui sont dirigées contre une infrastructure essentielle d'un État et contre les systèmes d'information correspondants. Le risque d'attaque grave de ce type est à la fois réel et sérieux.

6. Le risque que les technologies de l'information et des communications soient utilisées à des fins terroristes dans le cadre d'autres activités que le recrutement, le financement, l'entraînement et l'incitation au terrorisme, notamment contre des systèmes qui utilisent ces technologies ou contre des infrastructures qui en dépendent, augmente. Si l'on ne s'attaque pas à ce problème, il pourrait menacer la paix et la sécurité internationales.

7. La diversité des acteurs non étatiques malveillants, notamment les groupes criminels et les terroristes, leurs intentions diverses, la vitesse à laquelle des activités informatiques malveillantes peuvent être menées et la difficulté à déterminer l'origine d'un incident informatique contribuent à accroître le risque. Les États sont légitimement préoccupés par le danger de malentendus déstabilisateurs, par le risque de conflit et par l'éventualité de dommages pour leurs ressortissants, pour leurs biens et leur économie.

8. Les différences de capacités d'un État à un autre en matière de sécurité informatique peuvent aggraver la vulnérabilité d'un monde interconnecté.

III. Normes, règles, et principes de comportement responsable des États

9. Pour la communauté internationale, l'environnement informatique présente à la fois des perspectives et des difficultés pour déterminer comment des normes, des règles et des principes peuvent s'appliquer à l'utilisation de l'outil informatique par les États. L'un des objectifs consiste à établir de nouvelles normes facultatives et non contraignantes de comportement responsable des États et d'aboutir à une vision commune afin de renforcer la stabilité et la sécurité de l'environnement informatique mondial.

10. Des normes facultatives et non contraignantes de comportement responsable des États peuvent contribuer à réduire les risques qui pèsent sur la paix, la sécurité et la stabilité internationales. De ce fait, elles ne cherchent pas à limiter ou à interdire des actes qui respectent le droit international : elles traduisent les attentes de la communauté internationale, fixent des règles de comportement responsable des États et permettent à la communauté internationale d'étudier les activités menées par les États et d'apprécier leurs intentions. Ces normes peuvent servir à prévenir les conflits dans l'environnement informatique et contribuer à son utilisation pacifique, afin que les TIC puissent donner leur pleine mesure en vue d'accroître le développement économique et social à l'échelle mondiale.

11. Les rapports des précédents groupes d'experts faisaient état d'un consensus naissant sur le comportement responsable des États concernant la sécurité et l'utilisation des TIC qui résulte de normes et engagements internationaux existants. La tâche qui attendait le Groupe consistait à poursuivre l'examen des normes de comportement responsable des États, en vue de promouvoir l'adoption de vues communes, de déterminer dans quel domaine des normes existantes peuvent faire l'objet de développements afin de les rendre applicables à l'environnement informatique, d'encourager une meilleure acceptation des normes et de préciser dans quel domaine il pouvait être nécessaire d'élaborer des normes supplémentaires qui tiennent compte de la complexité et de la spécificité des technologies de l'information et des communications.

12. Le Groupe a pris note du code de conduite international pour la sécurité de l'information proposé par la Chine, la Fédération de Russie, le Kazakhstan, le Kirghizistan, l'Ouzbékistan et le Tadjikistan (document A/69/723).

13. En tenant compte des menaces, des risques et des failles réels ou naissants et en s'appuyant sur les constatations et les recommandations figurant dans les rapports des groupes d'experts de 2010 et de 2013, le Groupe actuel propose les

recommandations suivantes pour examen par les États concernant des normes, règles ou principes de comportement responsable des États facultatifs, non contraignants et devant permettre de promouvoir un environnement informatique ouvert, sûr, stable, accessible et pacifique :

a) Conformément aux buts des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, les États devraient coopérer à l'élaboration et à l'application de mesures visant à accroître la stabilité et la sécurité d'utilisation des TIC et à prévenir les pratiques informatiques jugées nocives qui peuvent compromettre la paix et la sécurité internationales;

b) En cas d'incident informatique, les États devraient examiner toutes les informations utiles, y compris le contexte plus large de l'événement, la difficulté de déterminer les responsabilités dans cet environnement et la nature et l'ampleur des conséquences de l'incident;

c) Les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications;

d) Les États devraient réfléchir à la meilleure façon de coopérer pour échanger des informations, s'assister mutuellement, engager des poursuites en cas d'utilisation terroriste ou criminelle des technologies de l'information et des communications et appliquer d'autres mesures collectives afin de parer à ces risques; à cet égard, les États peuvent être amenés à déterminer si de nouvelles mesures doivent être élaborées;

e) Les États, lorsqu'ils veillent à une utilisation sûre des technologies de l'information et des communications, devraient respecter les résolutions 20/8 et 26/13 du Conseil des droits de l'homme sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, ainsi que les résolutions 68/167 et 69/166 de l'Assemblée générale sur le droit à la vie privée à l'ère du numérique afin de garantir le plein respect des droits de l'homme, y compris le droit à la liberté d'expression;

f) Un État ne devrait pas mener ou soutenir sciemment une activité informatique qui est contraire aux obligations qu'il a contractées en vertu du droit international et qui endommage intentionnellement une infrastructure essentielle ou qui compromet l'utilisation et le fonctionnement d'une infrastructure essentielle pour fournir des services au public;

g) Les États devraient prendre les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux technologies de l'information et des communications en tenant compte de la résolution 58/199 de l'Assemblée générale sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information et d'autres résolutions pertinentes;

h) Les États devraient répondre aux demandes d'aide appropriées formulées par un autre État dont une infrastructure essentielle est exposée à des actes de malveillance informatique; ils devraient aussi répondre aux demandes appropriées visant à atténuer les conséquences d'activités informatiques malveillantes dirigées contre une infrastructure essentielle d'un autre État et exercées depuis leur territoire, en tenant dûment compte de la souveraineté;

i) Les États devraient prendre des mesures raisonnables pour garantir l'intégrité de la chaîne logistique, de sorte que les utilisateurs finaux puissent avoir confiance dans la sécurité des produits informatiques, et devraient s'attacher à prévenir la prolifération des techniques et des outils informatiques malveillants et l'utilisation de fonctionnalités cachées malveillantes;

j) Les États devraient encourager le signalement responsable des failles informatiques et partager les informations correspondantes sur les moyens permettant de les corriger, afin de limiter et éventuellement d'éliminer les risques pour les systèmes qui utilisent les technologies de l'information et des communications et pour les infrastructures qui en dépendent;

k) Les États ne devraient pas mener ou soutenir sciemment des activités visant à porter atteinte aux systèmes d'information des équipes d'intervention d'urgence agréées (parfois également appelées équipes d'intervention informatique d'urgence ou équipes d'intervention en cas d'atteinte à la sécurité informatique) d'un autre État; un État ne devrait pas se servir d'équipes d'intervention d'urgence agréées pour se livrer à des activités internationales malveillantes;

14. Le Groupe observe que ces mesures peuvent être essentielles pour promouvoir un environnement informatique ouvert, sûr, stable, accessible et pacifique, mais qu'il ne sera peut-être pas possible de les mettre en œuvre sans délai, en particulier dans les pays en développement, jusqu'à ce que ces derniers acquièrent les capacités suffisantes.

15. Compte tenu de la spécificité du domaine informatique, de nouvelles normes pourraient être élaborées au fil du temps.

IV. Mesures de confiance

16. Les mesures de confiance renforcent la paix et la sécurité internationales. Elles peuvent accroître la coopération, la transparence, la prévisibilité et la stabilité entre États. Lorsqu'ils cherchent à instaurer la confiance en vue de garantir un environnement informatique pacifique, les États devraient prendre en considération les principes directeurs pour l'élaboration de mesures de confiance, adoptés par la Commission du désarmement en 1988 et approuvé par consensus par l'Assemblée générale dans sa résolution 43/78 (point H). Afin d'accroître la confiance et la coopération et de réduire le risque de conflit, le Groupe recommande aux États de réfléchir aux mesures de confiance volontaires suivantes :

a) Recenser les points de contact appropriés aux niveaux décisionnel et technique pour parer aux graves incidents informatiques et créer un répertoire de ces contacts;

b) Concevoir et appuyer des mécanismes et procédures de concertation bilatérale, régionale, sous-régionale et multilatérale, selon qu'il conviendra, afin de renforcer la confiance entre États et de réduire le risque de malentendu, d'escalade et de conflit lié aux incidents informatiques;

c) Favoriser, à titre volontaire, la transparence à l'échelle bilatérale, sous-régionale, régionale et multilatérale, selon qu'il conviendra, afin d'accroître la confiance et d'éclairer les futurs travaux; cela peut se traduire par des échanges volontaires de vues et d'informations entre pays sur divers aspects des menaces

nationales et transnationales qui pèsent sur les technologies de l'information et des communications et sur leur utilisation : failles des produits informatiques et fonctionnalités cachées malveillantes qui ont été découvertes dans ces produits, meilleures pratiques relatives à la sécurité des systèmes informatiques, mesures de confiance élaborées dans des enceintes régionales ou multilatérales et organismes nationaux, stratégies, politiques et programmes qui intéressent la sécurité informatique;

d) Exposer volontairement leur point de vue sur les catégories d'infrastructures qu'ils jugent essentiels et sur les efforts engagés à l'échelle nationale pour les protéger, y compris des informations sur les lois et mesures nationales de protection des données et des infrastructures tributaires de systèmes informatiques; les États devraient s'attacher à faciliter la coopération transfrontière afin de s'attaquer aux failles des infrastructures essentielles qui transcendent les frontières nationales; ces mesures pourraient inclure :

i) La création d'un référentiel des lois et mesures de protection des données et des infrastructures tributaires de systèmes informatiques et la publication de documents sur ces lois et mesures jugés propres à être diffusés;

ii) La conception de mécanismes et de procédures de concertation bilatérale, régionale, sous-régionale et multilatérale pour la protection des données et des infrastructures essentielles qui sont tributaires de systèmes informatiques;

iii) L'élaboration de mécanismes techniques, juridiques et diplomatiques à l'échelle bilatérale, sous-régionale, régionale et multilatérale afin de traiter les demandes liées aux technologies de l'information et des communications;

iv) L'adoption de dispositifs volontaires nationaux pour classer les incidents informatiques en fonction de leur ampleur et de leur gravité, afin de faciliter les échanges d'informations sur les incidents.

17. Les États devraient envisager d'autres mesures de confiance qui renforceraient la coopération bilatérale, sous-régionale, régionale et multilatérale. Ces mesures pourraient comprendre le fait, pour les États, de convenir librement de :

a) Renforcer les mécanismes de coopération entre les organismes compétents pour parer aux incidents informatiques et élaborer de nouveaux mécanismes techniques, juridiques et diplomatiques pour traiter les demandes relatives aux infrastructures informatiques, y compris en envisageant des échanges de personnel dans des domaines comme les interventions en cas d'incident ou l'action répressive, selon qu'il conviendra, et encourager les échanges entre les institutions de recherche ou les établissements universitaires;

b) Renforcer la coopération, y compris en nommant des responsables pour l'échange d'informations sur l'utilisation malveillante des TIC et pour la fourniture d'assistance dans le cadre des enquêtes;

c) Constituer une équipe d'intervention informatique d'urgence ou une équipe d'intervention en cas d'atteinte à la sécurité informatique nationale ou désigner officiellement un organisme pour remplir ce rôle; les États pourront prendre en considération ces organes pour leur définition de l'infrastructure essentielle; ils devraient soutenir et faciliter le travail de ces équipes et la coopération entre celles-ci et d'autres organismes compétents;

d) Développer et appuyer les pratiques de coopération de l'équipe d'intervention informatique d'urgence ou de l'équipe d'intervention en cas d'atteinte à la sécurité informatique, selon le cas, par exemple les échanges d'informations sur les failles informatiques, les modèles d'attaque et les meilleures pratiques pour atténuer les conséquences des attaques, notamment les interventions coordonnées, l'organisation d'exercices, le soutien à la gestion des incidents informatiques et le renforcement de la coopération régionale et sectorielle;

e) Donner suite, dans le respect de la législation nationale et du droit international, aux demandes d'autres États pour enquêter sur des infractions liées aux technologies de l'information et des communications ou sur l'utilisation de ces technologies à des fins terroristes, ou pour atténuer les conséquences d'activités informatiques malveillantes exercées sur leur territoire;

18. Compte tenu de la vitesse à laquelle se développent les outils informatiques et de l'ampleur de la menace, le Groupe réaffirme qu'il est indispensable d'aboutir à des vues communes et d'intensifier la coopération. Pour ce faire, il recommande l'instauration d'un dialogue institutionnel régulier à large participation sous les auspices de l'Organisation des Nations Unies, ainsi que la mise en place d'un dialogue régulier au sein des instances bilatérales, régionales ou multilatérales et des autres organisations internationales.

V. Coopération et assistance internationales en matière de sécurité informatique et de renforcement des capacités

19. Les États sont responsables au premier chef de la sécurité nationale et de la sécurité de leurs ressortissants, mais certains États ne disposent peut-être pas de capacités suffisantes pour protéger leurs réseaux informatiques. Un manque de capacités peut rendre les ressortissants et les infrastructures essentielles d'un État vulnérables ou faire de ce dernier, sans qu'il le sache, un refuge pour des individus malintentionnés. La coopération et l'assistance internationales peuvent jouer un rôle essentiel pour permettre aux États de protéger leur environnement informatique et de garantir l'utilisation pacifique de ces technologies. La fourniture d'une assistance pour développer des capacités dans le domaine de la sécurité informatique est également indispensable pour la sécurité internationale, car elle permet d'améliorer les capacités des États en matière de coopération et d'action collective. Le Groupe estime que les mesures de renforcement des capacités devraient avoir pour objectif de promouvoir l'utilisation des technologies de l'information et des communications à des fins pacifiques.

20. Le Groupe a approuvé les recommandations sur le renforcement des capacités qui figurent dans les rapports de 2010 et de 2013. Le rapport de 2010 recommandait aux États de définir des moyens d'aider les pays moins avancés à renforcer leurs capacités, tandis que le rapport de 2013 appelait la communauté internationale à agir de concert afin de fournir une assistance pour améliorer la sécurité de leurs infrastructures informatiques essentielles, 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 concernant la sécurité et l'utilisation de leurs systèmes informatiques. Pour sa part, le Groupe actuel a souligné que le renforcement des capacités ne se résume pas à un transfert

de connaissances et de compétences des pays développés vers les pays en développement, car tous les États peuvent apprendre les uns des autres sur les risques auxquels ils sont exposés et sur les moyens efficaces d'y faire face.

21. Dans le prolongement des travaux engagés par des résolutions et des rapports approuvés par les Nations Unies, notamment la résolution 64/211 de l'Assemblée générale, intitulée « Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infostructures essentielles », les États devraient réfléchir aux mesures volontaires suivantes afin de fournir une assistance technique et autre pour permettre aux pays qui ont besoin d'aide et en font la demande de développer des capacités en vue de protéger leurs systèmes informatiques :

a) Contribuer à renforcer les mécanismes de coopération avec les équipes d'intervention informatique d'urgence nationales et d'autres organes compétents;

b) Fournir une assistance et offrir une formation aux pays en développement afin d'améliorer la sécurité d'utilisation des technologies de l'information et des communications, y compris en ce qui concerne les infrastructures essentielles, et échanger les meilleures pratiques législatives et administratives;

c) Aider à élargir l'accès aux technologies jugées essentielles pour la sécurité informatique;

d) Élaborer des procédures d'entraide pour intervenir en cas d'incident et résoudre des problèmes immédiats liés à la sécurité des réseaux, y compris des procédures d'assistance rapide;

e) Faciliter la coopération transfrontière afin de s'attaquer aux failles des infrastructures essentielles qui transcendent les frontières nationales;

f) Élaborer des stratégies pour pérenniser les efforts de renforcement des capacités en sécurité informatique;

g) Dans les plans et les budgets nationaux, placer la sensibilisation et le renforcement des capacités en matière de sécurité informatique parmi les priorités et leur accorder une importance appropriée dans la gestion prévisionnelle du développement et de l'assistance; cette mesure peut comprendre des programmes de sensibilisation à la sécurité informatique destinés à éclairer et à informer les organismes publics et les particuliers; ces programmes pourraient être couplés aux efforts engagés par des organisations internationales, notamment l'ONU et ses institutions, par le secteur privé, par le monde universitaire et par des organisations de la société civile;

h) Inciter à la poursuite des travaux en matière de renforcement des capacités, par exemple en ce qui concerne la criminalistique ou les mesures collectives visant à lutter contre l'utilisation criminelle ou terroriste des technologies de l'information et des communications.

22. L'élaboration de stratégies régionales pour renforcer les capacités serait bénéfique, car ces stratégies pourraient prendre en compte des aspects culturels, géographiques, politiques, économiques ou sociaux particuliers et s'y adapter.

23. Afin de renforcer les capacités en sécurité informatique, les États peuvent envisager de lancer des initiatives de coopération bilatérales et multilatérales qui

s'appuieraient sur des liens de partenariat existants. Ces initiatives favoriseraient une entraide efficace entre les États lorsqu'ils font face à un incident informatique et pourraient être enrichies par les organisations internationales compétentes, notamment l'ONU et ses institutions, par le secteur privé, par le monde universitaire et par des organisations de la société civile.

VI. Applicabilité du droit international à l'utilisation des TIC

24. Le rapport de 2013 affirmait que le droit international, et en particulier la Charte des Nations Unies, est applicable et essentiel pour maintenir la paix et la stabilité, ainsi que pour promouvoir un environnement informatique ouvert, sûr, stable, accessible et pacifique. Conformément à son mandat, le Groupe actuel a examiné l'applicabilité du droit international à l'utilisation des TIC par les États.

25. Le respect par les États du droit international, et en particulier de leurs obligations en vertu de la Charte, constitue un élément essentiel pour leur utilisation des TIC et pour promouvoir un environnement informatique ouvert, sûr, stable, accessible et pacifique. Ces obligations jouent un rôle central dans l'examen de l'application du droit international à l'utilisation des TIC par les États.

26. Lors de cet examen, le Groupe a jugé que les engagements des États à respecter les principes suivants de la Charte et d'autres principes de droit international étaient d'une importance centrale : égalité souveraine, règlement des différends internationaux par des moyens pacifiques, de telle manière que la paix et la sécurité internationales ainsi que la justice ne soient pas mises en danger, fait de s'abstenir, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies, respect des droits de l'homme et des libertés fondamentales et non-intervention dans les affaires intérieures d'autres États.

27. 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.

28. En s'appuyant sur les travaux des groupes précédents et guidé par la Charte et par le mandat défini par la résolution 68/243 de l'Assemblée générale, le Groupe actuel exprime les points de vue suivants, qui n'épuisent pas la question, sur l'applicabilité du droit international à l'utilisation des TIC par les États :

a) La compétence territoriale des États s'applique aux infrastructures informatiques situées sur leur territoire;

b) Lorsqu'ils utilisent les TIC, les États doivent respecter, entre autres principes du droit international, la souveraineté étatique, l'égalité souveraine, le règlement des différends par des moyens pacifiques et la non-intervention dans les affaires intérieures d'autres États; les obligations existantes qui découlent du droit international sont applicables à l'utilisation des TIC par les États; ces derniers doivent remplir l'obligation qui leur incombe en droit international de respecter et de protéger les droits de l'homme et les libertés fondamentales;

c) Soulignant les aspirations de la communauté internationale à l'utilisation pacifique des TIC pour le bien commun de l'humanité et rappelant que la Charte s'applique dans son intégralité, le Groupe a noté que les États avaient implicitement le droit de prendre des mesures conformes au droit international et reconnues par la Charte; il a convenu de la nécessité d'approfondir la question;

d) Le Groupe rappelle les principes de droit international reconnus, y compris, lorsqu'ils sont applicables, les principes d'humanité, de nécessité, de proportionnalité et de discrimination;

e) Les États ne doivent pas faire appel à des intermédiaires pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications et devraient veiller à ce que des acteurs non étatiques n'utilisent pas leur territoire pour commettre de tels actes;

f) Les États sont tenus de remplir leurs obligations internationales quant aux faits internationalement illicites qui leur sont imputables en droit international; néanmoins, le signe qu'une activité informatique a été lancée depuis le territoire ou une infrastructure informatique d'un État, ou y trouve son origine peut être insuffisant à lui seul pour imputer l'activité en question à cet État; le Groupe a fait observer que les accusations d'organiser et d'exécuter des actes illicites portées contre des États devaient être étayées.

29. Le Groupe a relevé que l'adoption des vues communes sur l'applicabilité du droit international à l'utilisation des TIC par les États est importante pour promouvoir un environnement informatique ouvert, sûr, stable, accessible et pacifique.

VII. Conclusions et recommandations pour les travaux futurs

30. Des progrès significatifs ont été accomplis dans la prise en compte des risques qui pèsent sur la paix et la sécurité internationales du fait de l'utilisation malveillante de l'informatique et des télécommunications. Sachant que ces outils peuvent être un puissant moteur de développement, et compte tenu de la nécessité de préserver au niveau mondial l'accès aux réseaux et la circulation de l'information en toute liberté et sécurité, le Groupe a estimé qu'il serait utile de recenser les mesures qui pourraient être prises en vue de travaux futurs. Elles comprennent notamment les suivantes, sans que cette liste soit nullement exhaustive :

a) Poursuite de la définition par les États, collectivement et individuellement, des éléments fondamentaux de la paix et de la sécurité internationales dans l'utilisation de l'informatique et des télécommunications sur les plans juridique et technique et en matière de politiques publiques;

b) Renforcement de la coopération aux niveaux régional et multilatéral en vue de promouvoir l'adoption de vues communes concernant les risques qui pourraient peser sur la paix et la sécurité internationales du fait de l'utilisation malveillante de l'informatique et des télécommunications, et concernant la sécurité des infrastructures essentielles informatisées.

31. C'est aux États qu'il incombe au premier chef de garantir un environnement informatique sûr et pacifique, mais la coopération internationale gagnerait en

efficacité si l'on mettait au point des mécanismes pour la participation du secteur privé, des milieux universitaires et de la société civile.

32. Parmi les domaines dans lesquels de plus amples travaux de recherche et d'étude pourraient être utiles figurent les questions ayant trait à l'utilisation de l'informatique et des télécommunications par les États. En sa qualité d'institut de recherche au service de tous les États membres, l'Institut des Nations Unies pour la recherche sur le désarmement pourrait être invité à entreprendre les études pertinentes, au même titre que d'autres groupes de réflexion et organismes de recherche.

33. L'ONU devait jouer un rôle moteur dans la promotion du dialogue sur la sécurité de l'utilisation que les États font de l'informatique et des télécommunications, ainsi que dans la définition de positions communes concernant l'application du droit international et des normes, règles et principes de comportement responsable des États. Dans les travaux futurs, on pourrait examiner des initiatives visant à lancer un dialogue international et des échanges de vues sur les problématiques de sécurité informatique. Il faudrait veiller à ce que ces efforts ne fassent pas double emploi avec les travaux d'autres organisations et instances internationales traitant de questions telles que l'utilisation des moyens informatiques à des fins criminelles et terroristes, les droits de l'homme et la gouvernance d'Internet.

34. Le Groupe a souligné l'importance que revêt l'examen consacré par l'Assemblée générale à la constitution d'un nouveau Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale en 2016, instance qui devrait poursuivre l'étude de ces questions en vue de favoriser l'émergence de vues communes sur les menaces qui existent ou pourraient exister dans le domaine de la sécurité de l'information et, éventuellement, les mesures de coopération à prendre pour y faire face, ainsi que sur la manière dont le droit international s'applique à l'utilisation de l'informatique et des télécommunications par les États, y compris les normes, règles ou principes de comportement responsable des États, les mesures de confiance et le renforcement des capacités.

35. Le Groupe salue les précieux efforts déployés par les organisations internationales et les groupes régionaux. Les États devraient tenir compte de ces avancées dans leur collaboration en matière de sécurité informatique et encourager, autant qu'il y a lieu, la constitution de plateformes bilatérales, régionales et multilatérales favorisant le dialogue, la concertation et le renforcement des capacités.

36. Le Groupe d'experts recommande aux États Membres d'examiner activement les recommandations formulées dans le présent rapport sur la manière d'aider à construire un environnement informatique ouvert, sûr, stable et pacifique, et d'évaluer la façon dont elles peuvent être approfondies et appliquées.

Annexe

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

Bélarus

Aliaksandr Chasnouski (troisième et quatrième sessions)
Chef adjoint du Département de la sécurité internationale et du contrôle des armements, Ministère des affaires étrangères

Ambassadeur Vladimir N. Gerasimovich (première session)
Chef du Département de la sécurité internationale et du contrôle des armements, Ministère des affaires étrangères

Ivan Grinevich (deuxième session)
Conseiller de la Mission permanente du Bélarus auprès de l'Organisation des Nations Unies, Genève

Brésil

Carlos Luís Dantas Coutinho Perez
Ministre, chef d'état-major du Vice-Ministre des affaires politiques, Ministère des relations extérieures

Chine

Haitao Wu (troisième et quatrième sessions)
Coordonnateur pour les questions relatives aux réseaux numériques, Ministère des affaires étrangères

Cong Fu (première et deuxième sessions)
Coordonnateur pour les questions relatives aux réseaux numériques, Ministère des affaires étrangères

Colombie

Jorge Fernando Bejarano
Directeur pour les normes et les réseaux numériques, Ministère des technologies de l'information et des communications

Égypte

Sameh Aboul-Enein
Ambassadeur, Ministre adjoint du désarmement, de la sécurité internationale et de l'utilisation de l'énergie nucléaire à des fins pacifiques, Ministère des affaires étrangères

Amr Aljowaily (troisième session)
Ministre, Mission permanente de l'Égypte auprès de l'Organisation des Nations Unies

Estonie

Marina Kaljurand
Sous-Secrétaire et conseillère juridique, Ministère des affaires étrangères

France

Florence Mangin
Ambassadrice, Coordinatrice pour la cybersécurité, Ministère des affaires étrangères

Léonard Rolland (première session)
Direction des affaires stratégiques, de sécurité et du désarmement,
Ministère des affaires étrangères

Allemagne

Karsten Geier
Responsable de l'équipe de coordination de la politique relative aux réseaux numériques, Ministère fédéral des affaires étrangères

Ghana

Mark-Oliver Kevor
Membre du conseil d'administration de l'Autorité nationale des communications

Israël

Iddo Moed
Coordonnateur pour la cybersécurité, Ministère des affaires étrangères

Japon

Takashi Okada (troisième et quatrième sessions)
Ambassadeur chargé des questions relatives à l'ONU et des questions de politique relatives aux réseaux numériques, Directeur général adjoint, Bureau de la politique étrangère, Ministère des affaires étrangères

Akira Kono (deuxième session)
Ambassadeur chargé des questions relatives à l'ONU et des questions de politique relatives aux réseaux numériques, Directeur général adjoint, Bureau de la politique étrangère, Ministère des affaires étrangères

Takao Imafuku (première session), négociateur principal pour les questions de sécurité internationale, Bureau de la politique étrangère, Ministère des affaires étrangères

Kenya

Katherine Getao
Secrétaire des technologies de l'information et des communications,
Ministère des technologies de l'information et des communications

Malaisie

Nur Hayuna Abd Karim (quatrième session)
Sous-secrétaire principale, Division de la cybersécurité et de la sécurité spatiale, Conseil national de sécurité

Md Shah Nuri bin Md Zain (première, deuxième et troisième sessions)
Sous-secrétaire, Division de la cybersécurité et de la sécurité spatiale, Conseil national de sécurité

Mexique

Edgar Zurita
Attaché auprès des États-Unis d'Amérique et du Canada, Commission de la sécurité nationale mexicaine – Police fédérale

Pakistan

Ausaf Ali (première, deuxième et quatrième sessions)
Directeur général, Service des questions techniques, Division des plans stratégiques, quartier général commun

Khalil Hashmi (troisième session)
Ministre, Mission permanente du Pakistan auprès de l'Organisation des Nations Unies

République de Corée

Chul Lee (deuxième et quatrième sessions)
Directeur, Division de la sécurité internationale, Ministère des affaires étrangères

Hyuncheol Jang (première et troisième sessions)
Conseiller de l'ambassade de la République de Corée au Royaume de Belgique et à l'Union européenne

Fédération de Russie

Andrey V. Krutskikh
Représentant spécial du Président de la Fédération de Russie pour la coopération internationale dans le domaine de la sécurité de l'information, Ambassadeur itinérant

Espagne

Ricardo Mor (quatrième session)
Ambassadeur itinérant pour la cybersécurité, Ministère des affaires étrangères et de la coopération

Alicia Moral (première, deuxième et troisième sessions)
Ambassadrice itinérante pour la cybersécurité, Ministère des affaires étrangères et de la coopération

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

Olivia Preston
Directrice adjointe, Bureau de la cybersécurité et de la protection des informations,
Cabinet du Premier Ministre

États-Unis d'Amérique

Michele G. Markoff
Coordonnatrice adjointe des questions relatives aux réseaux numériques,
Bureau du coordonnateur des questions relatives aux réseaux numériques,
Bureau du Secrétaire d'État, Département d'État