



Assemblée générale

Distr. limitée
22 octobre 2018
Français
Original : anglais

Soixante-treizième session

Première Commission

Point 96 de l'ordre du jour

**Progrès de l'informatique et des télécommunications
et sécurité internationale**

Algérie, Angola, Azerbaïdjan, Bélarus, Bolivie (État plurinational de), Burundi, Cambodge, Chine, Cuba, Érythrée, Fédération de Russie, Kazakhstan, Madagascar, Namibie, Népal, Nicaragua, Ouzbékistan, Pakistan, République arabe syrienne, République démocratique du Congo, République populaire démocratique de Corée, Samoa, Sierra Leone, Suriname, Tadjikistan, Venezuela (République bolivarienne du) et Zimbabwe : projet de résolution

**Progrès de l'informatique et des télécommunications
et sécurité internationale**

L'Assemblée générale,

Rappelant ses résolutions [36/103](#) du 9 décembre 1981, [43/78](#) H du 7 décembre 1988, [53/70](#) du 4 décembre 1998, [54/49](#) du 1^{er} décembre 1999, [55/28](#) du 20 novembre 2000, [56/19](#) du 29 novembre 2001, [57/53](#) du 22 novembre 2002, [58/32](#) du 8 décembre 2003, [59/61](#) du 3 décembre 2004, [60/45](#) du 8 décembre 2005, [61/54](#) du 6 décembre 2006, [62/17](#) du 5 décembre 2007, [63/37](#) du 2 décembre 2008, [64/25](#) du 2 décembre 2009, [65/41](#) du 8 décembre 2010, [66/24](#) du 2 décembre 2011, [67/27](#) du 3 décembre 2012, [68/243](#) du 27 décembre 2013, [69/28](#) du 2 décembre 2014, [70/237](#) du 23 décembre 2015 et [71/28](#) du 5 décembre 2016,

Notant que des progrès considérables ont été réalisés dans la conception et l'utilisation des technologies informatiques et des moyens de télécommunication de pointe,

Confirmant que les technologies de l'information et des communications sont des technologies à double usage et qu'elles peuvent être utilisées à la fois à des fins légitimes et malveillantes,

Se déclarant préoccupée par le fait que plusieurs États mettent au point des technologies de l'information et des communications à des fins militaires et que la probabilité que ces technologies soient utilisées dans des conflits futurs entre États augmente,

Soulignant qu'il est dans l'intérêt de tous les États de promouvoir l'utilisation des technologies de l'information et des communications à des fins pacifiques, l'objectif étant de bâtir pour l'humanité un avenir commun dans le cyberspace, et

* Nouveau tirage pour raisons techniques (24 octobre 2018).



qu'il est également dans leur intérêt de prévenir les conflits découlant de l'utilisation des technologies de l'information et des communications,

Notant que l'Organisation des Nations Unies devrait jouer un rôle de premier plan dans la promotion du dialogue entre les États Membres afin que ces derniers conviennent d'une position commune sur les questions liées à la sécurité et à l'utilisation des technologies de l'information et des communications, ainsi que dans la définition d'interprétations communes concernant l'application du droit international et de normes, règles et principes favorisant un comportement responsable des États dans ce domaine, encourager les efforts régionaux, favoriser les mesures de renforcement de la confiance et de transparence et appuyer le renforcement des capacités et la diffusion des meilleures pratiques,

Se déclarant préoccupée par le fait que l'incorporation aux technologies de l'information et des communications 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,

Jugeant nécessaire de prévenir l'utilisation des moyens et des technologies informatiques à des fins criminelles ou terroristes,

Soulignant qu'il importe de renforcer la coordination et la coopération entre États pour lutter contre l'exploitation des technologies de l'information à des fins criminelles, et insistant sur le rôle que l'Organisation des Nations Unies et d'autres organisations internationales et régionales peuvent jouer à cet égard,

Notant l'importance que revêt le respect des droits de l'homme et des libertés fondamentales dans l'utilisation des technologies de l'information et des communications,

Saluant les travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale ainsi que le rapport auquel ils ont abouti, qui lui a été transmis par le Secrétaire général¹,

Se félicitant de ce que, au cours de l'examen de l'application du droit international à l'utilisation des technologies de l'information et des communications par les États, le Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale ait jugé dans son rapport de 2015² 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,

Confirmant la conclusion à laquelle parvient le Groupe d'experts gouvernementaux dans ses rapports de 2013³ et 2015², à savoir que le droit international, et en particulier la Charte des Nations Unies, est applicable et essentiel au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies de l'information et des communications, que la mise en place, sur une base facultative et non

¹ A/65/201, A/68/98 et A/70/174.

² A/70/174.

³ A/68/98.

contraignante, de normes, règles et principes de comportement responsable des États en matière d'utilisation de ces technologies peut réduire les risques pesant sur la paix, la sécurité et la stabilité internationales et que, compte tenu de la spécificité de ces technologies, de nouvelles normes pourraient être progressivement élaborées,

Confirmant 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,

Notant que le renforcement des capacités est indispensable à la coopération entre les États et au renforcement de la confiance dans le domaine de la sécurité informatique,

Insistant sur la nécessité de redoubler d'efforts pour combler la fracture numérique en facilitant les transferts de technologies de l'information aux pays en développement dans les domaines des pratiques optimales et de la formation en matière de cybersécurité, conformément à 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 infrastructures essentielles »,

Soulignant que bien que ce soit aux États qu'il incombe au premier chef de garantir un environnement informatique sûr et pacifique, 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, selon qu'il conviendra,

1. *Se félicite* de l'adoption des normes, règles et principes internationaux de comportement responsable des États ci-après :

1. Les États doivent se conformer aux dispositions de la Charte des Nations Unies et aux normes universellement acceptées régissant les relations internationales qui consacrent, entre autres, le respect de la souveraineté, de l'intégrité territoriale et de l'indépendance politique de tous les États, le respect des droits de l'homme et des libertés fondamentales, de même que le respect de la spécificité de l'histoire, de la culture et du système social de chaque pays ;

2. Conformément aux buts des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, les États se doivent de coopérer à l'élaboration et à l'application de mesures visant à accroître la stabilité et la sécurité d'utilisation des technologies de l'information et des communications, et à prévenir les pratiques informatiques jugées nocives ou susceptibles de compromettre la paix et la sécurité internationales ;

3. Les États doivent s'abstenir d'utiliser les technologies et réseaux de l'information et des communications pour mener des activités incompatibles avec l'objectif du maintien de la paix et de la sécurité internationales ;

4. Les États doivent s'abstenir d'utiliser les technologies et réseaux de l'information et des communications pour s'ingérer dans les affaires intérieures d'autres pays ou compromettre leur stabilité politique, économique et sociale, et réaffirmer le droit et le devoir des États de lutter, dans les limites de leurs prérogatives constitutionnelles, contre la diffusion d'informations fausses ou déformées pouvant être interprétées comme une forme d'ingérence dans les affaires intérieures d'autres États ou comme étant préjudiciables à la promotion de la paix, de la coopération et des relations amicales entre les États et les nations ;

5. Les États doivent reconnaître le devoir de s'abstenir de toute campagne diffamatoire, de tout dénigrement ou de toute propagande hostile aux fins d'intervenir ou de s'ingérer dans les affaires intérieures d'autres États ;

6. Les États doivent s'efforcer d'assurer à tous les niveaux la sécurité de la chaîne logistique des produits et services liés aux technologies de l'information et des communications, afin d'empêcher d'autres États de profiter de leur position dominante dans le domaine informatique, notamment en ce qui concerne les ressources de base, les infrastructures critiques, les technologies essentielles, les produits et services liés aux technologies de l'information et des communications, et les réseaux correspondants, pour porter atteinte au droit des États de contrôler en toute indépendance lesdits produits et services ou menacer la sécurité politique, économique et sociale de ces États ;

7. Les États doivent réaffirmer les droits et les responsabilités de tous les États s'agissant de protéger, conformément aux lois et règles applicables, leur cyberspace et leurs infrastructures informatiques essentielles contre les menaces, ingérences, attaques et actes de sabotage ;

8. Les États doivent affirmer que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne ; respecter pleinement les droits et libertés dans le cyberspace, y compris le droit et la liberté de rechercher, d'acquérir et de diffuser des informations, tout en sachant que, selon l'article 19 du Pacte international relatif aux droits civils et politiques⁴, l'exercice de ces libertés comporte des devoirs spéciaux et des responsabilités spéciales et qu'il peut, en conséquence, être soumis à certaines restrictions qui doivent toutefois être expressément fixées par la loi et qui sont nécessaires :

- a) Au respect des droits ou de la réputation d'autrui ;
- b) À la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques ;

9. Tous les États doivent assumer le même rôle et la même responsabilité s'agissant d'assurer la gouvernance internationale d'Internet, d'en garantir la sécurité, la continuité et la stabilité, et de veiller à ce qu'il se développe d'une manière qui favorise la mise en place de mécanismes multilatéraux, transparents et démocratiques de gouvernance permettant d'assurer une répartition équitable des ressources, de faciliter l'accès de tous à Internet et d'assurer son fonctionnement stable et sûr ;

10. Les États sont tenus de remplir leurs obligations internationales quant aux faits internationalement illicites qui leur sont imputables en droit international. Toutefois, 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. Les États doivent noter que les accusations d'organiser et d'exécuter des actes illicites portées contre des États doivent être étayées. En cas d'incident informatique, les États doivent examiner toutes les informations pertinentes, y compris le contexte plus large de l'événement, la difficulté de déterminer les responsabilités dans le domaine des technologies de l'information et des communications et la nature et l'ampleur des conséquences ;

11. Les États ne doivent 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. Ils ne doivent pas faire appel à des

⁴ Voir résolution 2200 A (XXI), annexe.

intermédiaires pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications et doivent veiller à ce que des acteurs non étatiques n'utilisent pas leur territoire pour commettre de tels actes ;

12. Les États doivent réfléchir à la meilleure façon de coopérer pour échanger des informations, s'entraider, engager des poursuites en cas d'utilisation terroriste ou criminelle des technologies de l'information et des communications et faire obstacle à la diffusion d'informations incitant au terrorisme, au séparatisme ou à l'extrémisme ou attisant la haine ethnique, raciale ou religieuse ainsi que d'appliquer d'autres mesures collectives afin de parer à ces risques. Les États seront peut-être amenés à réfléchir à l'opportunité d'élaborer de nouvelles mesures dans ce domaine ;

13. Les États, lorsqu'ils veillent à une utilisation sûre des technologies de l'information et des communications, doivent respecter les résolutions 20/8 du 5 juillet 2012⁵ et 26/13 du 26 juin 2014⁶ 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 du 18 décembre 2013 et 69/166 du 18 décembre 2014 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 ;

14. Un État ne doit 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 ;

15. Les États doivent 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 du 23 décembre 2003 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 ;

16 Les États doivent répondre aux demandes d'aide appropriées formulées par un autre État dont une infrastructure essentielle est exposée à des actes de malveillance informatique. Ils doivent aussi répondre aux demandes 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 du principe de souveraineté ;

17. Les États doivent 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 le droit des États de gérer en toute indépendance les biens et services du domaine de l'informatique et des communications ne doit pas être mis en cause et leur sécurité politique, économique et sociale ne doit pas être menacée ;

18. Les États doivent s'attacher à prévenir la prolifération des techniques et des outils informatiques malveillants, et l'utilisation de fonctions cachées nuisibles ;

⁵ Voir *Documents officiels de l'Assemblée générale, soixante-septième session, Supplément n° 53 (A/67/53)*, chap. IV, sect. A.

⁶ *Ibid.*, *soixante-neuvième session, Supplément n°53 (A/69/53)*, chap. V, sect. A.

19. Les États doivent encourager le signalement responsable des failles informatiques et partager des informations correspondantes sur les moyens de les corriger afin de limiter voire d'éliminer les risques potentiels pour les systèmes qui utilisent les technologies de l'information et des communications et les infrastructures qui en dépendent ;

20. Les États ne doivent pas mener ou soutenir sciemment des activités visant à endommager les systèmes informatiques des équipes d'intervention d'urgence agréées (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 doit pas se servir d'équipes d'intervention d'urgence agréées pour se livrer à des activités internationales malveillantes ;

21. Les États doivent encourager le secteur privé et la société civile à jouer un rôle utile à l'appui du renforcement de la sécurité des technologies de l'information et des communications et de l'utilisation de celles-ci, y compris la sécurité de la chaîne logistique des produits et services informatiques. Les États doivent coopérer avec le secteur privé et les organisations de la société civile afin que ces derniers comprennent mieux le rôle potentiel qu'ils ont à jouer dans l'application des règles de comportement responsable dans le cyberspace ;

22. Les États doivent mettre en place, lorsque cela est possible et souhaitable, des mesures de confiance visant à accroître la prévisibilité et à réduire le risque de malentendus et de conflits, notamment : l'échange volontaire d'informations sur les stratégies et les structures institutionnelles existant au niveau national pour garantir la sécurité informatique de l'État, la publication de livres blancs et la mise en commun des meilleures pratiques ;

23. Les États doivent aider les pays en développement à renforcer leurs capacités en matière de sécurité informatique et à réduire la fracture numérique ;

24. Les États doivent renforcer la coopération bilatérale, régionale et internationale, aider l'Organisation des Nations Unies à jouer un rôle de premier plan dans des domaines tels que l'élaboration de normes de droit international relatives à la sécurité informatique, le règlement pacifique des différends internationaux et l'amélioration de la coopération internationale, en particulier dans le domaine de la sécurité informatique et renforcer la coordination entre les organisations internationales compétentes ;

25. Les États doivent régler tout différend résultant de l'application des normes, règles et principes internationaux de comportement responsable des États par des voies pacifiques et s'abstenir de recourir à la menace ou à l'emploi de la force ;

2. *Demande* aux États Membres de continuer de promouvoir au niveau multilatéral l'examen des menaces qui existent ou pourraient exister dans le domaine de la sécurité informatique, ainsi que des stratégies qui pourraient être adoptées pour y faire face, compte tenu de la nécessité de préserver la libre circulation de l'information ;

3. *Estime* que la poursuite de l'étude de principes internationaux destinés à renforcer la sécurité des systèmes informatiques mondiaux et des systèmes mondiaux de télécommunication pourrait permettre d'atteindre les buts de ces mesures ;

4. *Invite* tous les États Membres à continuer de communiquer au Secrétaire général, en tenant compte des constatations et recommandations figurant dans le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale¹, leurs vues et observations sur les questions suivantes :

- a) L'ensemble des questions qui se posent en matière de sécurité informatique ;
- b) Les actions engagées au niveau national pour renforcer la sécurité informatique et promouvoir la coopération internationale dans ce domaine ;
- c) Le contenu des principes visés au paragraphe 3 ci-dessus ;
- d) Les mesures que la communauté internationale pourrait prendre pour renforcer la sécurité informatique à l'échelle mondiale ;

5. *Prie* le Secrétaire général, en vue de rendre le processus de négociation de l'Organisation des Nations Unies sur la sécurité d'utilisation de l'informatique et des technologies des communications plus démocratique, inclusif et transparent, de poursuivre l'élaboration, à titre prioritaire, avec le concours d'un groupe de travail à composition non limitée qu'il constituera en 2019 et qui fonctionnera sur la base du consensus, de normes, règles et principes de comportement responsable des États visés au paragraphe 1 ci-dessus et de définir des moyens de les appliquer ; d'y apporter des changements ou d'en établir des nouveaux, selon qu'il conviendra ; d'étudier la possibilité d'instaurer un dialogue institutionnel régulier sous l'égide de l'Organisation des Nations Unies, aussi large que possible et 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, de la manière dont le droit international s'applique à l'utilisation de l'informatique et des technologies des communications par les États, ainsi que des normes, règles et principes de comportement responsable des États, des mesures de confiance et de renforcement des capacités, et des principes visés au paragraphe 3 de la présente résolution, en vue de définir une vision commune, de lui présenter à sa soixante-quinzième session un rapport sur les résultats de cette étude, et d'envisager, dans la limite des ressources et des contributions volontaires disponibles, la possibilité de tenir des réunions consultatives intersessions avec les parties intéressées, à savoir le secteur privé, les organisations non gouvernementales et le milieu universitaire, pour qu'ils puissent échanger leurs points de vue sur les questions relevant du mandat du groupe ;

6. *Décide* d'inscrire à l'ordre du jour provisoire de sa soixante-quatorzième session la question intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale ».