Nations Unies A/RES/73/27

Assemblée générale

Distr. générale
11 décembre 2018

Soixante-treizième session
Point 96 de l'ordre du jour

Résolution adoptée par l'Assemblée générale le 5 décembre 2018

[*sur la base du rapport de la Première Commission (A/73/505)*]

73/27. 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 1er 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 faits dans la conception et l'utilisation des technologies informatiques et des moyens de télécommunication de pointe,

Soulignant que la communauté internationale aspire à une utilisation pacifique des technologies numériques qui contribue au bien commun de l'humanité et favorise le développement durable de tous les pays, quel que soit leur niveau de développement scientifique et technique,

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 numérique,

Consciente que certains États peuvent avoir besoin d'une assistance pour concilier sécurité numérique et utilisation des technologies numériques,

Notant qu'il est essentiel, pour assurer la sécurité internationale, de fournir une aide au renforcement des capacités en matière de sécurité numérique à ceux qui en font la demande,

18-21207 (F)

Affirmant que les mesures de renforcement des capacités doivent promouvoir l'utilisation des technologies numériques à des fins pacifiques,

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

Se déclarant préoccupée par le fait que plusieurs États mettent au point des technologies numériques 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 du numérique à des fins pacifiques afin de bâtir pour l'humanité un avenir commun dans le cyberespace et qu'il est également dans leur intérêt de prévenir les conflits découlant de l'utilisation des technologies numériques,

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 ceux-ci conviennent d'une position commune sur les questions liées à la sécurité numérique et à l'utilisation des technologies numériques, 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 la dissimulation de fonctionnalités malveillantes dans les technologies numériques empêche d'utiliser celles-ci de façon sûre et fiable, dérègle la chaîne 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 l'importance que revêt le respect des droits de l'homme et des libertés fondamentales dans l'utilisation des technologies numériques,

Saluant les travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale ainsi que les rapports auxquels ils ont abouti, qui lui ont été transmis par le Secrétaire général[1],

Se félicitant que, au cours de l'examen de l'application du droit international à l'utilisation des technologies numériques par les États, le Groupe d'experts gouvernementaux ait jugé dans son rapport de 2015[2] que les engagements pris par les États de respecter les principes suivants de la Charte des Nations Unies 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, non-recours, dans les relations internationales, 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,

[1] A/65/201, A/68/98 et A/70/174.
[2] A/70/174.

Confirmant la conclusion à laquelle est parvenu le Groupe d'experts gouvernementaux dans ses rapports de 2013 [3] et 2015[2], 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 numérique ouvert, sûr, stable, accessible et pacifique, que la mise en place, sur une base facultative et non contraignante, de normes, règles et principes de comportement responsable des États en matière d'utilisation du numérique peut réduire les risques pesant sur la paix, la sécurité et la stabilité internationales et que, compte tenu de la spécificité du numérique, de nouvelles normes pourraient être progressivement élaborées,

Confirmant que la souveraineté étatique et les normes et principes internationaux qui procèdent de la souveraineté s'appliquent à l'utilisation du numérique par les États ainsi qu'à leur compétence territoriale en matière d'infrastructures numériques,

Réaffirmant 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,

Considérant que les États n'ont pas le droit de se livrer à des campagnes diffamatoires ou à des actes de dénigrement ou de propagande hostile aux fins d'intervenir ou de s'ingérer dans les affaires intérieures d'autres États,

Soulignant que bien que ce soit aux États qu'il incombe au premier chef de garantir un environnement numérique 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. *Accueille favorablement* les normes, règles et principes internationaux de comportement responsable des États ci-après, qui ont été énoncés et adoptés par consensus par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale dans ses rapports de 2013[3] et de 2015[2] et qui ont été recommandés dans la résolution 71/28, intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », qu'elle a adoptée le 5 décembre 2016 :

1.1. Conformément aux buts des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, les États coopèrent à l'élaboration et à l'application de mesures visant à accroître la stabilité et la sécurité d'utilisation des technologies numériques, et à prévenir les pratiques numériques jugées nocives ou susceptibles de compromettre la paix et la sécurité internationales.

1.2. Les États remplissent leurs obligations internationales quant aux faits internationalement illicites qui leur sont imputables en droit international. Toutefois, le signe qu'une activité numérique a été lancée depuis le territoire ou les infrastructures numériques d'un État ou y trouve son origine peut être insuffisant à lui seul pour imputer l'activité en question à cet État. Les accusations concernant l'organisation et l'exécution d'actes illicites portées contre des États doivent être étayées. En cas de problème, les États examinent toutes les informations pertinentes, y compris le contexte plus large de

[3] A/68/98.

l'événement, la difficulté de déterminer les responsabilités dans le domaine du numérique et la nature et l'ampleur des conséquences.

1.3. Les États ne permettent pas sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies numériques. Ils ne font pas appel à des intermédiaires pour commettre des faits internationalement illicites à l'aide des technologies numériques et veillent à ce que des acteurs non étatiques n'utilisent pas leur territoire pour commettre de tels actes.

1.4. Les États réfléchissent à la meilleure façon de coopérer pour échanger des informations, s'entraider et engager des poursuites en cas d'utilisation terroriste ou criminelle des technologies numériques et à la meilleure façon d'appliquer d'autres mesures collectives afin de parer à ces risques. Ils seront peut-être amenés à réfléchir à l'opportunité d'élaborer de nouvelles mesures dans ce domaine.

1.5. Les États, lorsqu'ils veillent à une utilisation sûre des technologies numériques, respectent les résolutions 20/8 et 26/13 du Conseil des droits de l'homme, en date du 5 juillet 2012[4] et du 26 juin 2014[5], sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, ainsi que les résolutions 68/167 et 69/166 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, qu'elle a adoptées l'une le 18 décembre 2013 et l'autre le 18 décembre 2014.

1.6. Un État ne mène ni ne soutient sciemment une activité numérique qui est contraire aux obligations qu'il a contractées en vertu du droit international et qui endommage intentionnellement des infrastructures essentielles ou qui compromet l'utilisation et le fonctionnement d'infrastructures essentielles à la fourniture de services au public.

1.7. Les États prennent les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux technologies numériques en tenant compte de sa résolution 58/199 du 23 décembre 2003 sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information et d'autres résolutions.

1.8. Les États répondent aux demandes d'aide que leur adressent d'autres États dont des infrastructures essentielles sont exposées à des actes de malveillance numérique, sous réserve que ces demandes soient justifiées. Ils donnent également suite aux demandes visant à atténuer les conséquences d'activités numériques malveillantes dirigées contre des infrastructures essentielles d'un autre État qui sont exercées depuis leur territoire, en tenant dûment compte du principe de souveraineté.

1.9. Les États prennent des mesures raisonnables pour garantir l'intégrité de la chaîne d'approvisionnement, de sorte que les utilisateurs finaux puissent avoir confiance dans la sécurité des produits numériques.

1.10. Les États s'attachent à prévenir la prolifération des techniques et des outils numériques malveillants et l'utilisation furtive de fonctionnalités néfastes.

1.11. Les États encouragent le signalement responsable des failles numériques et se communiquent des informations sur les moyens de les corriger afin de

[4] Voir *Documents officiels de l'Assemblée générale, soixante-septième session, Supplément nº 53* (A/67/53), chap. IV, sect. A.

[5] Ibid., *soixante-neuvième session, Supplément nº 53* (A/69/53), chap. V, sect. A.

limiter voire d'éliminer les risques potentiels pour les systèmes et les infrastructures qui utilisent les technologies numériques ou en dépendent.

1.12. Les États s'abstiennent de mener ou de 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 du cyberespace) d'un autre État. Un État ne doit pas se servir d'équipes d'intervention d'urgence agréées pour se livrer à des actes de malveillance au niveau international.

1.13. Les États incitent le secteur privé et la société civile à s'associer au renforcement de la sécurité numérique et à l'utilisation des technologies numériques, y compris pour ce qui est de la sécurité de la chaîne d'approvisionnement en produits et services numériques et coopèrent avec eux afin de mieux leur faire comprendre la manière dont ils peuvent faciliter l'application de règles de comportement responsable dans le cyberespace ;

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 numérique, et celui 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 et des systèmes de télécommunication au niveau mondial pourrait aider à 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 qui figurent 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 internationale[1], leurs vues et observations sur les questions suivantes :

a) L'ensemble des questions qui se posent en matière de sécurité numérique ;

b) Les mesures prises au niveau national pour renforcer la sécurité numérique et promouvoir la coopération internationale dans ce domaine ;

c) Les principes visés au paragraphe 3 ci-dessus ;

d) Les mesures que la communauté internationale pourrait prendre pour renforcer la sécurité numérique au niveau mondial ;

5. *Décide*, en vue de rendre le processus de négociation de l'Organisation des Nations Unies sur la sécurité d'utilisation du numérique plus démocratique, inclusif et transparent, de constituer à partir de 2019 un groupe de travail à composition non limitée qui sera chargé, sur la base du consensus, de poursuivre l'élaboration, à titre prioritaire, des règles, normes et principes de comportement responsable des États visés au paragraphe 1 de la présente résolution 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 aussi large que possible sous l'égide de l'Organisation des Nations Unies ; de poursuivre l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité numérique et des mesures de coopération qui pourraient être prises pour y parer, de la manière dont le droit international s'applique à l'utilisation du numérique 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 parvenir à

une vision commune ; de lui présenter à sa soixante-quinzième session un rapport sur les résultats de cette étude ; d'envisager, dans la limite 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 les milieux universitaires, pour qu'ils puissent échanger leurs vues sur les questions relevant du mandat du groupe ;

6. *Décide* que le groupe de travail à composition non limitée tiendra sa session d'organisation en juin 2019 afin de déterminer ses modalités de fonctionnement ;

7. *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 ».

45e séance plénière
5 décembre 2018