Nations Unies A/69/723

Assemblée générale

Distr. générale
13 janvier 2015
Français
Original : anglais

Soixante-neuvième session
Point 91 de l'ordre du jour
Progrès de l'informatique et des télécommunications et sécurité internationale

Lettre datée du 9 janvier 2015, adressée au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie, du Kazakhstan, du Kirghizistan, de l'Ouzbékistan et du Tadjikistan auprès de l'Organisation des Nations Unies

Au cours des dernières années, des progrès considérables ont été faits dans la mise au point et l'application de nouvelles technologies de l'information et des communications, qui risquent toujours d'être utilisées à des fins contraires à l'objectif du maintien de la paix et de la sécurité internationales. Un consensus se dégage actuellement sur la nécessité de renforcer la coopération à l'échelle mondiale et d'élaborer les normes qui s'imposent afin de parer aux dangers qui menacent la communauté internationale dans le domaine de la sécurité de l'information. C'est ainsi qu'en 2011, la Chine, l'Ouzbékistan, la Russie et le Tadjikistan ont présenté à l'Assemblée générale, à sa soixante-sixième session, le Code de conduite international pour la sécurité de l'information qu'ils avaient élaboré conjointement et dont le Kirghizistan et le Kazakhstan se sont portés coauteurs ultérieurement. Distribué comme document de l'Assemblée générale sous la cote A/66/359, ce code de conduite a suscité un vif intérêt et de longs débats. Nous l'avons donc révisé en prenant en compte les observations et suggestions formulées par l'ensemble des parties. Nous avons à présent l'honneur de faire tenir ci-joint les versions anglaise, chinoise et russe du code ainsi révisé (voir annexe). Nous espérons ainsi faire avancer le débat sur les normes internationales de sécurité de l'information et contribuer à recueillir bientôt un consensus sur cette question.

Nous vous serions très reconnaissants de bien vouloir faire distribuer le texte de la présente lettre et de son annexe comme document de la soixante-neuvième session de l'Assemblée générale, au titre du point 91 de l'ordre du jour.

Le Représentant permanent
de la République populaire de Chine
auprès de l'Organisation des Nations Unies
(*Signé*) **Liu** Jieyi

15-00392 (F) 220115 220115

Le Représentant permanent
de la Fédération de Russie
auprès de l'Organisation des Nations Unies
(*Signé*) Vitaly **Churkin**

Le Représentant permanent
de la République du Kazakhstan
auprès de l'Organisation des Nations Unies
(*Signé*) Kairat **Abdrakhmanov**

Le Représentant permanent
de la République kirghize
auprès de l'Organisation des Nations Unies
(*Signé*) Talaibek **Kydyrov**

Le Représentant permanent
de la République d'Ouzbékistan
auprès de l'Organisation des Nations Unies
(*Signé*) Muzaffarbek **Madrakhimov**

Le Représentant permanent
de la République du Tadjikistan
auprès de l'Organisation des Nations Unies
(*Signé*) Mahmadamin **Mahmadaminov**

Annexe à la lettre datée du 9 janvier 2015 adressée au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie, du Kazakhstan, du Kirghizistan, de l'Ouzbékistan et du Tadjikistan auprès de l'Organisation des Nations Unies

[Original : chinois et russe]

Code de conduite international pour la sécurité de l'information

L'Assemblée générale,

Se référant à ses résolutions sur le rôle de la science et de la technique dans le contexte de la sécurité internationale et du désarmement, dans lesquelles elle constate notamment que les progrès de la science et de la technique doivent avoir une application à la fois civile et militaire et qu'il faut soutenir et encourager l'essor de ces domaines d'activité à des fins civiles,

Se référant également à ses résolutions intitulées « Progrès de l'informatique et des télécommunications et sécurité internationale », à savoir les résolutions 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 et 68/243 du 27 décembre 2013,

Notant que des progrès importants ont été faits dans l'élaboration et la mise en œuvre de technologies de pointe en matière d'information et de communications,

Constatant qu'il faut empêcher que les technologies de l'information et des communications soient utilisées à des fins incompatibles avec l'objectif du maintien de la paix et de la sécurité internationales et susceptibles de menacer l'intégrité des infrastructures publiques en compromettant leur sécurité,

Soulignant qu'il est nécessaire de renforcer la coordination et la coopération entre les États dans la lutte contre l'utilisation des technologies de l'information à des fins criminelles, et notant le rôle que peuvent jouer, à cet égard, l'Organisation des Nations Unies et d'autres organisations internationales et régionales,

Soulignant qu'il importe qu'Internet fonctionne de manière sûre, continue et stable et qu'il faut le protéger, comme les autres réseaux d'information et de communication, contre les menaces, et affirmant qu'il convient d'arrêter une conception commune de la sécurité d'Internet et de continuer à coopérer à l'échelle nationale et internationale,

Réaffirmant que les décisions touchant aux questions de politique publique relatives à Internet relèvent du droit souverain des États, qui ont des droits et des devoirs en la matière à l'échelle internationale,

Prenant note des observations et des recommandations figurant dans le rapport final du Groupe d'experts gouvernementaux créé en 2012, en application de la résolution 66/24, dans le respect du principe de répartition géographique équitable,

qui a étudié, dans le cadre de son mandat, les dangers qui menaçaient ou risquaient de menacer la sécurité de l'information et les mesures conjointes qu'il serait possible de prendre pour les écarter, notamment l'adoption de normes, règles ou principes de conduite responsable pour les États ou de mesures destinées à renforcer la fiabilité des systèmes informatiques, et réfléchi aux principes internationaux qui pourraient contribuer à renforcer la sécurité des systèmes mondiaux d'information et de télécommunications,

Affirmant, conformément au paragraphe 16 du rapport du Groupe d'experts gouvernementaux en date du 24 juin 2013 (A/68/98), qu'il faut déterminer collectivement comment les normes découlant du droit international en vigueur, dont l'application est un préalable indispensable à la réduction des risques qui pèsent sur la paix, la sécurité et la stabilité internationales, doivent s'appliquer à la conduite des États et à l'utilisation qu'ils font des technologies de l'information et des communications,

Notant que, compte tenu des particularités des technologies de l'information et des communications, d'autres normes pourront être élaborées progressivement, conformément au paragraphe 16 du rapport du Groupe d'experts gouvernementaux,

Estimant que la fiabilité et la sécurité de l'utilisation des technologies de l'information et des communications sont les piliers de la société de l'information et qu'il faut encourager, élaborer, développer et mettre en œuvre un solide cadre mondial de cybersécurité, conformément aux dispositions de sa résolution 64/211 intitulée « Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infostructures essentielles »,

Notant, comme dans sa résolution 64/211, qu'il faut redoubler d'efforts pour combler la fracture numérique en facilitant le transfert des technologies de l'information et des communications vers les pays en développement et en aidant ces pays à se doter de moyens accrus pour élaborer des pratiques de référence et des outils pédagogiques dans le domaine de la cybersécurité,

Adopte le code de conduite ci-après, qui régit la sécurité internationale de l'information :

I. But et champ d'application

Le présent Code de conduite a pour but de définir les droits et les responsabilités des États dans le cyberespace, d'encourager ceux-ci à s'y comporter de manière constructive et responsable, et de renforcer leur coopération pour faire face aux menaces et défis communs qu'ils y rencontrent, afin de créer un cyberespace qui soit pacifique, sûr, ouvert et coopératif, et de faire en sorte que l'utilisation des technologies et des réseaux de l'information et des communications contribue au plein développement social et économique et au bien-être des peuples, et soit conforme à l'objectif du maintien de la stabilité et de la sécurité internationales.

L'adhésion au présent Code de conduite est volontaire et ouverte à tous les États.

II. Code de conduite

Tout État adhérant volontairement au présent Code de conduite s'engage :

1. À 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. À ne pas 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;

3. À ne pas 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;

4. À coopérer pour lutter contre les activités criminelles et terroristes menées à l'aide des technologies et réseaux de l'information et des communications, et à faire obstacle à la diffusion d'informations incitant au terrorisme, au sécessionnisme, à l'extrémisme ou à la haine nationale, raciale ou religieuse;

5. À s'efforcer d'assurer 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;

6. À réaffirmer les droits et les responsabilités de tous les États s'agissant de protéger, conformément aux lois et règles applicables, leur cyberespace et leurs infostructures essentielles contre les menaces, ingérences, attaques et actes de sabotage;

7. À affirmer que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne; à respecter pleinement les droits et libertés dans le cyberespace, y compris le droit et la liberté de rechercher, d'acquérir et de diffuser des informations, tout en sachant que, selon le Pacte international relatif aux droits civils et politiques (art. 19), 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;

8. À assumer le même rôle et la même responsabilité que les autres États s'agissant d'assurer la gouvernance d'Internet, de garantir la sécurité, la continuité

et la stabilité de ce dernier, 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 d'Internet qui permettent d'assurer une répartition équitable des ressources, de faciliter l'accès de tous et d'assurer le fonctionnement stable et sûr d'Internet;

9. À coopérer pleinement avec les autres parties intéressées et à promouvoir dans toutes les composantes de la société, y compris le secteur privé et les institutions de la société civile, une meilleure compréhension de leur rôle et de leurs responsabilités en ce qui concerne la sécurité de l'information, notamment en facilitant l'instauration d'une culture de la sécurité de l'information et en concourant à la protection des infostructures essentielles;

10. À mettre en place des mesures de confiance – notamment, dans la mesure du possible et selon qu'il convient, l'échange volontaire d'informations sur les stratégies nationales et les structures institutionnelles destinées à sauvegarder la sécurité de l'information du pays, la publication de livres blancs et la mise en commun des pratiques optimales – propres à améliorer la prévisibilité, à éviter les malentendus et à réduire les risques de conflit;

11. À aider les pays en développement à renforcer leurs capacités en matière de sécurité de l'information et à réduire la fracture numérique;

12. À renforcer la coopération bilatérale, régionale et internationale, à aider l'ONU à jouer un rôle important dans des domaines tels que la promotion de l'élaboration de normes de droit international relatives à la sécurité de l'information, le règlement pacifique des différends internationaux et l'amélioration de la coopération internationale, en particulier dans le domaine de la sécurité de l'information, et à renforcer la coordination entre les organisations internationales compétentes;

13. À régler tout différend résultant de l'application du présent Code de conduite par des voies pacifiques et à s'abstenir de recourir à la menace ou à l'emploi de la force.