Nations Unies S/2021/540

Conseil de sécurité

Distr. générale
8 juin 2021
Français
Original : anglais

Lettre datée du 8 juin 2021, adressée au Secrétaire général par le Représentant permanent de l'Estonie auprès de l'Organisation des Nations Unies

L'Estonie, qui exerce la présidence du Conseil de sécurité pour le mois de juin 2021, prévoit d'organiser, le mardi 29 juin 2021 à 8 heures (heure d'été de New York), un débat public sur le thème « Préserver la paix et la sécurité internationales dans le cyberespace », au titre de la question « Maintien de la paix et de la sécurité internationales ».

Afin d'encadrer les débats sur le sujet, l'Estonie a établi la note ci-jointe (voir annexe).

Je vous serais reconnaissant de bien vouloir faire distribuer le texte de la présente lettre et de son annexe comme document du Conseil de sécurité.

L'Ambassadeur,
Représentant permanent
(*Signé*) Sven **Jürgenson**

Annexe à la lettre datée du 8 juin 2021 adressée au Secrétaire général par le Représentant permanent de l'Estonie auprès de l'Organisation des Nations Unies

Note de cadrage pour le débat public du Conseil de sécurité sur le thème « Préserver la paix et la sécurité internationales dans le cyberespace », qui se tiendra le 29 juin 2021

I. Objectif

1. Ce débat public vise à mieux faire connaître les risques croissants liés aux activités malveillantes sur Internet et les conséquences de ces dernières sur la paix et la sécurité internationales, et à permettre aux participants d'examiner les actions menées au niveau mondial pour promouvoir la paix et la stabilité dans le cyberespace. Les États Membres auront l'occasion de réaffirmer leur engagement en faveur du droit international et du cadre de comportement responsable des États en tant qu'éléments clés de la prévention des conflits et du maintien de la paix et de la sécurité sur Internet.

II. Contexte

2. Conformément à la Charte des Nations Unies, la responsabilité première du Conseil de sécurité est le maintien de la paix et de la sécurité internationales. En conséquence, le Conseil a suivi de près l'évolution des menaces pesant sur la sécurité internationale en examinant un certain nombre de facteurs nouveaux et complexes susceptibles de déstabiliser des pays et d'exacerber ou de prolonger des conflits existants. Au fil des ans, il a tenu de vastes débats thématiques sur les nouvelles menaces pour la paix et la sécurité internationales, ainsi que des réunions consacrées à des questions spécifiques, telles que les changements climatiques, les ressources naturelles, les pandémies, la famine, la criminalité transnationale organisée, le trafic de drogues et la piraterie.

3. Si le Conseil de sécurité abordera pour la première fois de manière distincte la question de la cybersécurité à l'occasion de ce débat public, il a précédemment abordé ce sujet dans le cadre de réunions informelles et d'un débat plus large sur la sécurité internationale. Ces réunions ont montré que, pour de nombreux pays, les cybermenaces sont un sujet de préoccupation et constituent un problème de sécurité majeur. En décembre 2017, par exemple, sous la présidence du Japon, le Conseil a tenu un débat public consacré à la lutte contre les problèmes contemporains complexes pesant sur la paix et la sécurité internationales. À cette occasion, le Secrétaire général a pointé la cybersécurité comme l'une des menaces croissantes pour la paix et la sécurité internationales (voir S/PV.8144). En août 2019, la Pologne a organisé un débat public consacré aux menaces contre la paix et la sécurité au Moyen-Orient, invitant les participants à réfléchir aux moyens de « contrer les cybermenaces, y compris les menaces visant l'infrastructure énergétique, en promouvant des mécanismes de coopération propres à décourager les cyberincidents majeurs au Moyen-Orient et à y réagir » (voir S/2019/643), question que plusieurs d'entre eux ont abordée dans leurs interventions. Plus récemment, en avril 2021, sous la présidence du Viet Nam, plusieurs participants au débat de haut niveau sur la question « Protection des civils en période de conflit armé : biens de caractère civil indispensables » (voir S/2021/415), y compris des personnes ayant présenté des exposés, ont souligné les menaces que les cyberactivités malveillantes faisaient peser sur les infrastructures critiques, notamment les installations médicales.

4. Un cyberespace libre, ouvert et interopérable, géré et soutenu par une communauté multipartite, a de toute évidence permis aux États de dégager des profits considérables et de promouvoir le progrès social à l'échelle mondiale. Les technologies numériques sont un important catalyseur du progrès et du développement de l'humanité. Elles sont en outre un moyen important de promouvoir le respect des droits humains, en permettant aux groupes vulnérables et marginalisés de la société de s'exprimer. Le développement numérique durable peut par ailleurs contribuer de manière significative à la promotion de la stabilité post-conflit dans les zones de conflit régional.

5. Parallèlement à la dépendance croissante à l'égard du numérique et aux divers avantages offerts par la transformation numérique, on constate malheureusement une augmentation continue des activités malveillantes sur Internet ainsi que des menaces systémiques croissantes qui perturbent le fonctionnement d'infrastructures critiques et de services numériques. L'utilisation abusive du cyberespace peut affecter des secteurs économiques vitaux et des services essentiels au public, tels que les soins de santé et l'énergie. Cela pourrait avoir un impact humanitaire potentiellement dévastateur et provoquer une instabilité susceptible de menacer la paix et la sécurité internationales. La pandémie provoquée par la maladie à coronavirus (COVID-19) a encore accru la dépendance à l'égard des infrastructures numériques critiques, soulignant l'importance d'un comportement responsable des États dans le cyberespace, conformément aux principes du droit international.

6. Pour réduire l'utilisation malveillante des cybercapacités et stabiliser le cyberespace, il est absolument indispensable de suivre les mécanismes préventifs applicables aux niveaux mondial, régional et national. Au cours de la dernière décennie, les États Membres de l'Organisation des Nations Unies ont fait des progrès remarquables dans la formulation des éléments d'un cadre normatif pour un comportement responsable des États dans le cyberespace, fondé sur le droit international existant, les normes, les mesures de confiance et le renforcement des capacités.

7. Le droit international existant, notamment la Charte, fournit aux États des orientations suffisantes pour mener leurs activités sur Internet. Les principes du droit international qui ont permis de régler le comportement des États dans d'autres domaines constituent également un cadre de référence essentiel pour les États en ce qui concerne l'utilisation du cyberespace. Outre le droit international, les normes volontaires et non contraignantes de comportement responsable des États en temps de paix et les mesures de confiance jouent également un rôle crucial en fournissant des orientations sur le comportement des États dans le cyberespace, améliorant ainsi la transparence, la clarté et la prévisibilité. Les États sont tenus de remplir leurs obligations quant aux faits internationalement illicites qui leur sont imputables en droit international.

8. Les groupes d'experts gouvernementaux successifs créés dans le cadre de la Première Commission de l'Assemblée générale ont examiné la question de la promotion d'un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et produit des rapports de consensus en 2010, 2013, 2015 et 2021[1]. L'Assemblée générale des États Membres de l'ONU a décidé par consensus de s'inspirer, pour ce qui touchait aux technologies numériques, des normes de comportement responsable des États, ainsi que du droit international et des mesures de confiance[2]. Le succès des processus numériques mis en œuvre au sein de la Première Commission en 2021 incite à appliquer plus largement encore le cadre

[1] Les rapports publiés sous les cotes A/65/201, A/68/98 et A/70/174 ont été approuvés par l'Assemblée générale ; le rapport qui a été examiné le 28 mai 2021 n'a pas encore été publié.

[2] Résolution 70/237 de l'Assemblée générale.

pour un comportement responsable des États dans le cyberespace. Le rapport de consensus adopté par le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui a été approuvé par l'Assemblée générale, réaffirme l'application du droit international dans le cyberespace, les normes, les mesures de confiance et le renforcement des capacités[3]. Le rapport de consensus issu de la dernière réunion en date du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale a permis, dans une large mesure, de mieux comprendre l'application du droit international à l'utilisation des technologies numériques par les États, en donnant des orientations supplémentaires sur la mise en œuvre des normes, ainsi qu'en favorisant la confiance et le renforcement des capacités dans le cyberespace.

9. Des organisations régionales telles que l'Organisation des États américains, l'Organisation pour la sécurité et la coopération en Europe, l'Union africaine, l'Association des nations de l'Asie du Sud-Est (ASEAN) et le Forum régional de l'ASEAN ont également fait des progrès considérables en adoptant des accords régionaux relatifs à la cybersécurité ainsi qu'en élaborant et en appliquant des mesures de renforcement de la cyberconfiance visant à contribuer à la stabilité et à réduire la probabilité d'une escalade vers un conflit. En parallèle, le travail accompli en matière de renforcement des capacités et le large éventail de programmes mondiaux et régionaux qui ont été mis en place jouent un rôle essentiel dans l'amélioration de la cyberrésilience. En outre, étant donné que les États n'ont pas tendance à gérer eux-mêmes l'ensemble de leurs infrastructures critiques, mais qu'ils s'appuient sur la coopération avec le secteur privé, un certain nombre d'initiatives public-privé en matière de cybersécurité ont vu le jour. Compte tenu de la nature multipartite du cyberespace, il convient d'encourager davantage toute possibilité d'associer le secteur privé, les milieux universitaires et la société civile aux discussions tenues aux niveaux mondial, régional et national.

III. Questions d'orientation

10. Les États Membres pourraient traiter des questions ci-après dans leurs interventions dans le cadre du débat :

a) Quelles cybermenaces actuelles et nouvelles pèsent sur la paix et la sécurité internationales ? Quelles pourraient être les conséquences d'une utilisation malveillante du cyberespace sur les conflits ?

b) De quels mécanismes politiques dispose-t-on aux niveaux mondial, régional et national pour atténuer les cybermenaces et promouvoir un comportement responsable des États, et comment les États Membres de l'ONU peuvent-ils encourager efficacement leur mise en œuvre ?

c) Comment renforcer le respect du droit international et l'application des normes de comportement responsable des États dans le cyberespace, comme convenu par l'Assemblée générale des Nations Unies ?

d) Comment renforcer la confiance, réduire les malentendus et prévenir les cyberactivités malveillantes susceptibles d'avoir des effets dévastateurs sur le plan humanitaire ?

[3] Décision 75/564 de l'Assemblée générale.

e) Comment atténuer les risques humanitaires liés à l'utilisation malveillante des technologies numériques dans le cadre des conflits armés ?

f) Compte tenu de la nature multipartite du cyberespace, quel rôle les acteurs non étatiques, notamment le secteur privé, la société civile et le monde universitaire, peuvent-ils jouer pour aider à prévenir les conflits, à arrêter des interprétations communes et à accroître la cyberrésilience ?

g) Si une situation grave découlant de cyberactivités est susceptible d'entraîner un conflit international ou de donner lieu à un différend, de quelles options dispose-t-on pour y répondre et rechercher une solution pacifique ?

IV. Intervenant(e)s

11. La Haute-Représentante pour les affaires de désarmement a été invitée à présenter un exposé au Conseil.

V. Format

12. Le débat public de haut niveau se tiendra le 29 juin 2021 sous la forme d'une visioconférence publique. Il sera présidé par la Première Ministre de la République d'Estonie, Kaja Kallas.

13. Les États Membres de l'Organisation des Nations Unies qui ne sont pas membres du Conseil de sécurité et les observateurs permanents auprès de l'Organisation sont invités à déposer des déclarations écrites par l'intermédiaire du module e-Speakers. Les États Membres qui souhaitent faire une déclaration écrite sont priés de bien vouloir la transmettre au format Microsoft Word, accompagnée d'une lettre de couverture dûment signée par le (la) représentant(e) permanent(e) ou chargé(e) d'affaires et adressée au Président du Conseil de sécurité, au plus tard à la date de la séance, le 29 juin 2021. Les déclarations seront publiées dans un document officiel contenant les interventions soumises au titre du débat public par visioconférence.