Nations Unies S/2020/389

Conseil de sécurité

Distr. générale
12 mai 2020
Français
Original : anglais

Lettre datée du 12 mai 2020, adressée au Secrétaire général par le Représentant permanent de l'Estonie auprès de l'Organisation des Nations Unies

J'ai l'honneur de vous informer que l'Estonie compte tenir une réunion du Conseil de sécurité selon la formule Arria, sur le thème « Cyberstabilité, prévention des conflits et renforcement des capacités », qui aura lieu le 22 mai 2020, de 10 à 13 heures, par visioconférence. La note de cadrage y relative est jointe à la présente lettre (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**

20-06648 (F) 150520 150520

Annexe à la lettre datée du 12 mai 2020 adressée au Secrétaire général par le Représentant permanent de l'Estonie auprès de l'Organisation des Nations Unies

Note de cadrage relative à la réunion organisée selon la formule Arria sur le thème « Cyberstabilité, prévention des conflits et renforcement des capacités », qui se tiendra le 22 mai 2020

Réunion organisée par la Mission permanente de l'Estonie auprès de l'Organisation des Nations Unies, en collaboration avec les Missions permanentes de la Belgique, de l'Indonésie, du Kenya et de la République dominicaine auprès de l'Organisation des Nations Unies

Objectif

1. L'objectif de cette réunion organisée selon la formule Arria est d'offrir aux membres du Conseil de sécurité une possibilité d'examiner les efforts déployés à l'échelle internationale en vue de mieux stabiliser le cyberespace et de prévenir les conflits dans le contexte des cybermenaces qui se font jour. Ce sera l'occasion de renforcer la sensibilisation aux problèmes qui se posent en la matière sous l'angle de la paix et de la sécurité internationales et de se pencher, notamment, sur les mécanismes d'intervention mis en place aux niveaux mondial, régional et national pour réduire les cybermenaces et favoriser un comportement responsable des États.

Contexte

2. La connectivité mondiale connaît une croissance rapide. Avec 4,33 milliards d'internautes et 26 milliards d'appareils connectés, l'écosystème numérique mondial se développe à un rythme sans précédent. L'accélération de la numérisation a ouvert de multiples possibilités à l'ensemble de nos sociétés et l'on ne saurait trop insister sur les avantages du développement de la connectivité sur les plans économique et social. Par ailleurs, l'expansion rapide du domaine numérique a entraîné une dépendance critique par rapport au bon fonctionnement des services et infrastructures numériques. Ces dernières années, la multiplication et l'aggravation des cyberattaques et des incidents, en perturbant le fonctionnement des infrastructures critiques et des services numériques, ont contribué à rendre plus incertaine la situation internationale sur le plan de la sécurité. À la montée des cybermenaces correspond un risque croissant d'instabilité et de conflit. Dans le cadre de la crise sanitaire mondiale actuelle, la nécessité de protéger des infrastructures médicales critiques ainsi que les ressources Internet mondiales souligne toute l'importance d'un renforcement de la sécurité et de la stabilité dans le cyberespace.

3. Pour réduire l'utilisation malveillante des cybercapacités et stabiliser le cyberespace, il est absolument indispensable de suivre les mécanismes préventifs et normatifs applicables aux niveaux mondial, régional et national. Au cours des dix dernières années, les instances intergouvernementales et multipartites ont été nombreuses à inscrire au programme de leurs débats internationaux la question de la responsabilité des comportements dans le cyberespace. L'Assemblée générale a entériné les normes régissant le comportement responsable des États et l'application du droit international au cyberespace. Les organisations régionales se sont attelées à l'élaboration de mesures de confiance dans le domaine numérique, destinées à renforcer la stabilité et à réduire le risque que des problèmes dégénèrent en conflit. Plusieurs initiatives public-privé ont vu le jour dans le domaine de la cybersécurité et la question du rôle des nouvelles technologies dans la sécurité internationale fait son chemin dans les grands débats de politique étrangère.

4. Les États Membres de l'ONU ont déjà accompli des progrès remarquables dans la formulation des éléments d'un cadre de prévention des conflits et de renforcement de la stabilité dans le cyberspace. Les groupes d'experts consécutifs créés sous l'égide 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 trois rapports dont l'Assemblée générale a pris note avec satisfaction en 2010, 2013 et 2015[1]. En 2015, dans la résolution 70/237, l'Assemblée générale a décidé par consensus de s'inspirer, pour ce qui touche à l'utilisation de l'informatique et des technologies des communications, des normes de comportement responsable des États. Les délibérations en cours à la Première Commission et dans les deux groupes créés sous son égide – le Groupe d'experts gouvernementaux et le Groupe de travail à composition non limitée – contribuent à l'application des normes de comportement responsable des États et du droit international ainsi qu'au renforcement des capacités et de la confiance.

5. Un certain nombre d'organisations régionales, telles que l'Organisation des États américains, l'Organisation pour la sécurité et la coopération en Europe, l'Union africaine et l'Association des nations de l'Asie du Sud-Est, ont sensiblement progressé dans l'adoption d'accords régionaux sur la cybersécurité et de mesures de confiance. Certaines, comme l'Organisation des États américains, sont également à l'avant-garde des efforts menés pour promouvoir la cyberrésilience à l'échelon national et développer les capacités techniques et institutionnelles de lutte contre les cybermenaces. La communauté internationale s'accorde sur la nécessité de redoubler d'efforts en matière de renforcement des capacités afin de parer au risque d'attaques contre des infrastructures critiques et de développer les compétences politiques et techniques voulues pour sécuriser l'économie numérique. Accroître la cyberrésilience au niveau des pays, pour leur permettre de faire face aux cybermenaces, c'est poser les premières briques de la cyberstabilité mondiale.

6. Le respect du droit international dans le cyberespace est un autre élément fondamental de la cyberstabilité et de la prévention des conflits. Les principes du droit international qui ont permis de régler le comportement des États dans d'autres domaines constituent également, dans le cyberespace, un cadre de référence essentiel pour le comportement des États. Le droit international peut fournir des orientations sur le type de conduite considéré comme acceptable, dans le cyberespace, de la part des États et contribuer ainsi à rendre plus clair et plus prévisible le comportement de ces derniers. Le droit international contient également un ensemble de principes sur lesquels on peut s'appuyer pour renforcer la cyberrésilience des infrastructures critiques.

7. Dans le prolongement de la réunion de 2016 organisée selon la formule Arria par les Missions permanentes de la République du Sénégal et de l'Espagne auprès de l'Organisation des Nations Unies, sur le thème « Cybersécurité et paix et sécurité internationales », on voit la nécessité d'approfondir ce débat sous l'angle de la prévention des conflits. Alors que les cyberdébats se poursuivent à l'Organisation des Nations Unies sous une variété de formats, cette réunion programmée sur le thème « Cyberstabilité, prévention des conflits et renforcement des capacités » aura pour but de renforcer la sensibilisation sur la question du comportement responsable des États dans le cyberespace. Le débat portera sur les normes, politiques et mécanismes de coopération actuels pouvant permettre de promouvoir la cyberstabilité, la prévention des conflits et le renforcement des capacités aux niveaux mondial, régional et national.

[1] Voir www.un.org/disarmament/ict-security/.

Intervenantes et intervenants

- La Secrétaire générale adjointe et Haute-Représentante pour les affaires de désarmement
- M. James Lewis, Premier Vice-Président et Directeur du Programme politique technologique au Centre d'études stratégiques internationales
- M. David Koh, Directeur général de l'Office de la cybersécurité de Singapour

Questions devant servir à orienter le débat

8. Les États Membres pourront s'appuyer sur les questions ci-après pour préparer leur déclaration :

a) Comment les États Membres de l'ONU ont-ils mis en œuvre jusqu'à présent le cadre de cyberstabilité que constituent les normes volontaires de comportement responsable adoptées par les États, les mesures de confiance et le droit international ?

b) Quelles mesures préventives les États pourraient-ils prendre pour favoriser un comportement responsable des États dans le cyberespace afin de créer des conditions préalables viables pour une prévention efficace des conflits découlant des cyber-risques ?

c) Quel type d'action régionale concourt-il à l'observation par les États de normes de comportement responsable et à la mise en œuvre de mesures de confiance, et par voie de conséquence, à la cyberstabilité et à la prévention des conflits ? Quelles sont les actions les plus notables menées à l'échelon régional en matière de lutte contre les cybermenaces ?

d) Quels mécanismes mondiaux et régionaux existants permettent d'avoir une meilleure compréhension et une vue d'ensemble des actions menées en matière de renforcement des capacités ? Comment pourrait-on organiser le renforcement des capacités de manière plus efficace compte tenu du besoin urgent de renforcer la cyber-résilience au niveau national dans de nombreux États Membres ? Quels sont les critères appliqués pour le renforcement des cybercapacités dans les différentes régions ?

Modalités

9. La réunion sera présidée par le Représentant permanent de l'Estonie auprès de l'Organisation des Nations Unies, Sven Jürgenson. Après la déclaration liminaire, prononcée par le Premier Ministre estonien, Jüri Ratas, les intervenants présenteront leur exposé. La parole sera ensuite donnée aux co-organisateurs et aux représentants des États membres du Conseil de sécurité, qui pourront faire une brève déclaration. Si le temps le permet, les représentants des autres États Membres de l'ONU, des observateurs permanents et des organisations non gouvernementales pourront intervenir. Les délégations ayant l'intention de prendre la parole doivent l'indiquer dans le formulaire d'inscription, à renvoyer avant le 18 mai 2020 à l'adresse : EEUNSC@mfa.ee. Les interventions des représentants des États Membres, des observateurs permanents et des organisations non gouvernementales ne devront pas dépasser trois minutes. Les contributions écrites sont également bienvenues ; elles seront insérées dans le compte-rendu de la réunion.

10. La réunion organisée selon la formule Arria se déroulera sous la forme d'une visioconférence, diffusée en direct sur YouTube, Facebook et sur le site Web de la Mission permanente de l'Estonie auprès de l'Organisation des Nations Unies. Le détail exact des modalités sera communiqué sous peu. Les consignes et indications

techniques permettant de participer à la réunion seront communiquées aux intervenants inscrits avant la date limite.