



Conseil de sécurité

Distr. générale
10 juin 2024
Français
Original : anglais

Lettre datée du 7 juin 2024, adressée au Président du Conseil de sécurité par le Représentant permanent de la République de Corée auprès de l'Organisation des Nations Unies

J'ai l'honneur de vous faire tenir ci-joint la lettre d'invitation au débat public de haut niveau du Conseil de sécurité sur le thème « Maintien de la paix et de la sécurité internationales : faire face à l'évolution des menaces dans le cyberspace », qui se tiendra le jeudi 20 juin 2024 à 10 heures, ainsi que la note de cadrage correspondante (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 de la République de Corée
auprès de l'Organisation des Nations Unies
(Signé) Joonkook Hwang



**Annexe à la lettre datée du 7 juin 2024 adressée au Président du
Conseil de sécurité par le Représentant permanent de la
République de Corée auprès de l'Organisation des Nations Unies**

J'ai le plaisir de vous inviter au débat public de haut niveau du Conseil de sécurité sur le thème « Maintien de la paix et de la sécurité internationales : faire face à l'évolution des menaces dans le cyberspace », qui se tiendra le jeudi 20 juin, à 10 heures, dans la salle du Conseil de sécurité (voir la note de cadrage). Il s'agira de la manifestation phare de la présidence du Conseil par la République de Corée au mois de juin.

Dans un contexte où les technologies de l'information et des communications font des progrès rapides, porteurs d'avantages mais aussi de problèmes dans notre monde hyperconnecté, les cyberactivités malveillantes, sophistiquées et intrusives, suscitent de vives inquiétudes pour la paix et la sécurité internationales. À cet égard, l'évolution du paysage de la cybersécurité exige du Conseil qu'il accorde une attention particulière à la lutte contre les cybermenaces qui peuvent toucher toutes les nations.

Le débat public de haut niveau sera présidé par le Ministre des affaires étrangères de la République de Corée, Cho Tae-yul, et constituera pour le Conseil une occasion précieuse de s'acquitter de sa mission principale, le maintien de la paix et de la sécurité internationales, à l'ère où les cybermenaces prennent de plus en plus d'ampleur. Une participation de haut niveau à cette manifestation enrichira considérablement les débats.

Le Représentant permanent
(*Signé*) Joonkook **Hwang**

Note de cadrage en vue du débat public de haut niveau sur le thème « Maintien de la paix et de la sécurité internationales : faire face à l'évolution des menaces dans le cyberspace », 20 juin 2024, 10 heures

Contexte

Si les progrès de l'informatique et des communications sont porteurs d'énormes avantages économiques, sociaux, culturels, civils et politiques, notre forte dépendance à l'égard de l'infrastructure numérique pour la communication, le commerce et la gouvernance a pour effet d'exposer la paix et à la sécurité internationales aux risques de la cybermalveillance, qui peut frapper simultanément dans plusieurs domaines.

Les cyberactivités malveillantes visant les infrastructures critiques, notamment les hôpitaux et autres systèmes de santé, les services financiers, le secteur de l'énergie, les satellites, les transports et d'autres systèmes d'urgence, sont de plus en plus courantes. Elles peuvent avoir des effets dévastateurs sur la sécurité nationale et représenter un véritable risque pour les civils. Non seulement ces activités prolifèrent, mais les tactiques évoluent et se perfectionnent (rançongiciels leurres, plateformes de location de rançongiciels, vols de cryptomonnaie destinés à financer des activités terroristes, des programmes d'armes nucléaires et d'autres armes de destruction massive...) et rendent la menace de plus en plus complexe, ce qui est encore aggravé par l'introduction de nouveaux vecteurs d'attaque et de nouvelles vulnérabilités à exploiter.

Si les cyberactivités malveillantes sont évidentes dans toute une série de contextes, l'utilisation des technologies du numérique dans le cadre de conflits armés et à l'appui de ceux-ci est particulièrement inquiétante. Les cyberactivités malveillantes peuvent à la fois aggraver les situations de conflit existantes et favoriser l'apparition de nouvelles tensions.

Compte tenu de la nature transnationale du cyberspace, aucun État n'est à l'abri des dégâts de la cybermalveillance. La solidité du réseau de cybersécurité se mesure à celle de son maillon le plus faible. Aussi le renforcement des capacités est-il un élément indispensable de la coopération entre toutes les instances qui traitent des questions liées à l'informatique et aux communications dans le système des Nations Unies. Les différences de capacités ou de résilience cybernétique posent des problèmes supplémentaires lorsqu'il s'agit de détecter les cyberactivités malveillantes, s'en défendre ou y faire face, en particulier pour les États dont les capacités sont insuffisantes. Un usage des technologies de l'information et des communications à des fins préjudiciables peut avoir des effets disproportionnés sur certaines populations, notamment les femmes et les minorités.

Le rôle du Conseil de sécurité

Progrès accomplis

Depuis une dizaine d'années, le Conseil de sécurité est de plus en plus souvent saisi de la question des implications du cyberspace pour la paix et la sécurité internationales. Depuis 2016, il a organisé plusieurs réunions selon la formule Arria, au cours desquelles les États ont abordé la cybersécurité en l'associant à des questions telles que la protection des infrastructures critiques, la protection des civils, ainsi que la désinformation et les discours de haine dans le cyberspace. L'Estonie a organisé le premier débat public de haut niveau sur le sujet en 2021, consolidant encore la place de la problématique du maintien de la paix et de la sécurité internationales dans le cyberspace au rang des questions dont est saisi le Conseil.

La dernière réunion sur la cybersécurité organisée selon la formule Arria l'a été par la République de Corée, avec le concours des États-Unis et du Japon, en avril 2024. Elle a permis de mettre en évidence les implications de plus en plus fortes des cybermenaces dans le contexte de la paix et de la sécurité internationales, ainsi que l'importance du rôle du Conseil de sécurité dans la désescalade des tensions et la promotion de la cybersécurité.

Options envisageables

Il est aujourd'hui essentiel de travailler à une compréhension commune entre les États et de renforcer le rôle du Conseil de sécurité dans la lutte contre les cybermenaces. Une participation proactive à la cybersécurité, qui cadre avec la responsabilité première qui est la sienne de maintenir la paix et la sécurité internationales, met le Conseil en position d'offrir une réponse aux cyberactivités malveillantes et de contribuer ainsi fortement à faire du cyberspace un espace mondial sûr, ouvert et pacifique, dans l'intérêt de toutes les nations.

La participation du Conseil de sécurité peut se faire en complément d'autres processus engagés par les Nations Unies concernant l'informatique et les communications, notamment les discussions sur les normes de comportement responsable des États dans l'utilisation des technologies de l'information et des communications, ainsi que le cadre de comportement responsable des États dans le cyberspace, qui a été adopté par consensus, sous les auspices de l'Assemblée générale.

Lors de la réunion organisée selon la formule Arria, en avril, des options ont été présentées au Conseil pour examen, l'objectif étant de contribuer utilement aux diverses mesures multilatérales qui traitent des conséquences des cyberactivités malveillantes sur la paix et la sécurité internationales.

Le Conseil de sécurité pourrait par exemple envisager d'organiser une séance d'information, idéalement à intervalles réguliers, consacrée à l'évolution des cybermenaces et à leur incidence sur son mandat et sur les questions dont il est saisi. En analysant ces menaces et en élaborant des stratégies d'intervention, avec l'éclairage du système des Nations Unies, du secteur privé, de la société civile et du monde universitaire, le Conseil pourrait rester au fait des dernières évolutions et de leurs conséquences sur la paix et la sécurité internationales.

Compte tenu de la nature transversale des menaces pour la paix et la sécurité internationales provenant du cyberspace, le Conseil pourrait également étudier les moyens de tenir compte des préoccupations liées au cyberspace ou aux technologies de l'information et des communications lorsqu'il examine des dossiers portant sur tel ou tel pays ou des questions thématiques, tels que les missions de maintien et de consolidation de la paix, les sanctions imposées par le Conseil, les femmes et la paix et la sécurité, ou la non-prolifération et la lutte contre le terrorisme. L'amélioration de la résilience cybernétique, le renforcement des capacités nationales en matière de cybersécurité et la promotion de la coopération internationale pourraient également être intégrés dans chacun de ces axes d'action.

En outre, les États Membres de l'Organisation pourraient étudier les moyens de renforcer la capacité du Conseil de sécurité de réagir face aux utilisations malveillantes des technologies de l'information et des communications qui mettent en péril la paix et la sécurité internationales, notamment celles qui menacent la protection des civils, les infrastructures essentielles et l'action humanitaire, afin de garantir une approche plus globale du maintien de la paix et de la sécurité.

Questions devant servir à orienter le débat

Les questions suivantes peuvent aider à orienter les interventions des États Membres :

- Quelles sont les principales tendances nouvelles de la cybermalveillance qui menacent la paix et la sécurité internationales ?
- En quoi l'utilisation malveillante des technologies de l'information et des communications est-elle « multiplicatrice de menace » dans les conflits en cours et dans le cadre des problèmes existants, d'une manière qui nécessite l'action du Conseil de sécurité ?
- Quel rôle le Conseil de sécurité peut-il jouer et quelles mesures peut-il prendre pour relever les défis concernant la paix et la sécurité internationales que pose le cyberspace, et comment ce rôle peut-il évoluer dans le cadre de son mandat, de manière que ses travaux renforcent et complètent ceux d'autres organismes des Nations Unies ? Quelles sont les prochaines étapes qui s'imposent ?
- Comment les cybermenaces sont-elles liées à d'autres questions dont est saisi le Conseil de sécurité ? Comment le Conseil peut-il intégrer efficacement les préoccupations liées au numérique ou aux technologies de l'information et des communications dans ses travaux actuels ?

Modalités et intervenantes et intervenants

Le débat public de haut niveau sera présidé par M. Cho Tae-yul, Ministre des affaires étrangères de la République de Corée, et les membres du Conseil sont encouragés à s'y faire représenter au niveau ministériel. Afin de permettre au plus grand nombre possible de délégations de participer, les interventions ne devront pas dépasser trois minutes.

Les personnes ci-après prendront la parole devant le Conseil de sécurité :

- Le Secrétaire général de l'Organisation des Nations Unies, António Guterres ;
- Stéphane Duguin, Directeur exécutif du CyberPeace Institute ;
- Nnenna Ifeanyi-Ajufo, professeur de droit et technologie, Université Beckett de Leeds (Royaume-Uni).

La liste des orateurs et des oratrices du débat public sera ouverte à 9 h 30 le 14 juin, le troisième jour ouvrable précédant la date de la réunion. Pour y être inscrit, il faudra télécharger dans le module eSpeakers du portail e-deleGATE une lettre adressée à la présidence du Conseil de sécurité, dûment signée par le (la) représentant(e) permanent(e) ou chargé(e) d'affaires par intérim et contenant une demande de participation au titre de l'article 37 du Règlement intérieur provisoire du Conseil.