Nations Unies S/PV. 9662 (Resumption 1)

Conseil de sécurité

Soixante-dix-neuvième année

Provisoire

9662e séance
Jeudi 20 juin 2024, à 15 heures
New York

Président :	M. Hyunwoo Cho	(République de Corée)
Membres :	Algérie	M. Louafi
	Chine	M. Wang Zhenjiang
	Équateur	M. Durán Medina
	États-Unis d'Amérique	Mme Wu
	Fédération de Russie	M. Dergachev
	France	M. Strehaiano
	Guyana	Mme Parmanand
	Japon	M. Suzuki
	Malte	M. Ciscaldi
	Mozambique	M. Irachande Gouveia
	Royaume-Uni de Grande-Bretagne et d'Irlande du Nord	Mme Page
	Sierra Leone	M. Schenks
	Slovénie	M. Burkeljc
	Suisse	M. Stritt

Ordre du jour

Maintien de la paix et de la sécurité internationales

Faire face à l'évolution des menaces dans le cyberespace

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 (S/2024/446)

Ce procès-verbal contient le texte des déclarations prononcées en français et la traduction des autres déclarations. Le texte définitif sera publié dans les *Documents officiels du Conseil de sécurité*. Les rectifications éventuelles ne doivent porter que sur le texte original des interventions. Elles doivent être indiquées sur un exemplaire du procès-verbal, porter la signature d'un membre de la délégation intéressée et être adressées au Chef du Service de rédaction des procès-verbaux de séance, bureau AB-0928 (verbatimrecords@un.org). Les procès-verbaux rectifiés seront publiés sur le Système de diffusion électronique des documents de l'Organisation des Nations Unies (http://documents.un.org)

24-17609 (F)

Document adapté

Merci de recycler

La séance est reprise à 15 h 5.

Le Président (*parle en anglais*) : Je rappelle aux orateurs et oratrices qu'ils sont priés de limiter la durée de leurs déclarations à un maximum de trois minutes afin que le Conseil puisse mener ses travaux avec diligence. Le voyant rouge de leur microphone se mettra à clignoter au bout de trois minutes pour les inviter à conclure.

Je donne maintenant la parole au représentant de Cuba.

M. Gala López (Cuba) (*parle en espagnol*) : L'utilisation des technologies de l'information et des communications doit être réservée à des fins exclusivement pacifiques, dans l'intérêt de la coopération et du développement des peuples.

Cuba s'oppose fermement à la militarisation du cyberespace et à toute utilisation des technologies de l'information et des communications comme instruments de menace ou de recours à la force, ou pour des actions d'ingérence dans les affaires intérieures des États. L'Article 51 de la Charte des Nations Unies ne s'applique pas et ne saurait être invoqué dans le contexte du cyberespace. Il est inquiétant de constater que certains États incluent dans leurs stratégies de sécurité nationale l'utilisation de cyberarmes et la possibilité de mener des cyberattaques, soi-disant pour dissuader les adversaires.

Il faut prendre toutes les mesures qui s'imposent pour empêcher l'utilisation abusive des technologies de l'information et des communications et des plateformes de médias, y compris les réseaux sociaux, les émissions de radio et les transmissions électroniques, comme outils de promotion des discours de haine, d'incitation à la violence, de subversion, de déstabilisation, de diffusion de fausses nouvelles et de déformation de la réalité des États à des fins subversives et d'ingérence, en violation du droit international. L'utilisation clandestine et illégale des systèmes informatiques nationaux par des individus, des organisations et des États pour mener des cyberattaques contre des pays tiers est également inacceptable.

Cuba préconise la négociation, dans le cadre de l'ONU, et l'adoption, dans les meilleurs délais, d'un instrument international juridiquement contraignant qui permettra de combler les lacunes juridiques importantes en matière de cybersécurité et de faire face efficacement aux défis et menaces croissants dans ce domaine, notamment grâce à la coopération internationale. Il est nécessaire de combler l'énorme fossé technologique actuel et d'éliminer les obstacles imposés aux pays en développement s'agissant d'investir dans la sécurité de leurs infrastructures de technologies de l'information et des communications, qui limitent leur capacité à faire face aux menaces.

Le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), qui a été créé par la Première Commission de l'Assemblée générale, est le mécanisme approprié pour mener des échanges et parvenir à un accord sur les menaces et les défis auxquels les États sont confrontés en ce qui concerne l'utilisation malveillante des technologies de l'information et des communications. Le groupe est un forum inclusif, démocratique et transparent au sein duquel tous les États Membres peuvent contribuer, sur un pied d'égalité, à l'élaboration de solutions consensuelles dans ce domaine.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante de Bahreïn.

M^me^ Salman (Bahreïn) (*parle en arabe*) : Je tiens tout d'abord à souhaiter la bienvenue à S. E. M. Cho Tae-yul, Ministre des affaires étrangères de la République de Corée, qui a présidé la partie du débat public qui a eu lieu ce matin, et à remercier la Mission permanente de la République de Corée auprès de l'Organisation des Nations Unies d'avoir organisé la présente séance sur un sujet qui revêt une importance croissante, compte tenu des évolutions majeures en lien avec le cyberespace. Je tiens également à remercier S. E. M. António Guterres, Secrétaire général de l'Organisation des Nations Unies, et les autres intervenants de leurs précieuses déclarations.

Les risques croissants posés par les cyberactivités malveillantes, telles que les attaques par rançongiciels, le vol de cryptomonnaie et le vol d'informations et d'actifs sensibles, mettent non seulement en péril la sécurité des infrastructures critiques, mais exacerbent également les défis existants pour la stabilité mondiale. Ces activités sont de puissants multiplicateurs de menace, qui amplifient les problèmes de sécurité traditionnels et créent de nouvelles vulnérabilités. La nature interconnectée des systèmes numériques signifie que les cyberincidents peuvent rapidement dégénérer en crises internationales, sapant la confiance entre les États et leur stabilité.

Le Royaume de Bahreïn souligne l'importance d'une approche multidimensionnelle, qui consiste notamment à tirer parti des outils, plateformes, cadres et stratégies innovants actuels pour atténuer les risques liés aux cybermenaces, ainsi qu'à associer toutes les parties prenantes, étant donné que les cyberoutils et les cybertechnologies ne relèvent plus du domaine exclusif des gouvernements. Le Royaume de Bahreïn souligne

également l'importance du renforcement des capacités et du partage des technologies, des connaissances et des meilleures pratiques afin d'améliorer la capacité des États de prévenir les cyberincidents et d'y répondre.

Dans ce contexte, le Royaume de Bahreïn a appuyé diverses initiatives de l'Assemblée générale visant à renforcer la coopération aux fins du maintien de la cybersécurité, notamment les groupes d'experts gouvernementaux, le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), et le programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale.

Au niveau national, le Royaume de Bahreïn attache une grande importance à la cybersécurité, fondée sur un système de gouvernance de la cybersécurité clair, soutenu par une stratégie nationale globale. Nous avons également créé le Centre national de cybersécurité pour assurer la sécurité du cyberespace dans le Royaume de Bahreïn en établissant des normes de gouvernance efficaces, en fournissant des moyens de défense contre les attaques électroniques, en les surveillant et en y ripostant, ainsi qu'en sensibilisant les personnes et les institutions.

La stratégie nationale de cybersécurité renforce les partenariats régionaux et internationaux. Cinq piliers fondamentaux ont été définis dans le cadre de cette stratégie, et chacun d'entre eux est un élément essentiel et nécessaire à la concrétisation de la vision du Royaume de Bahreïn en matière de cybersécurité. Ensemble, ils forment un cadre complet et cohérent pour le maintien d'un cyberespace sûr et fiable. Ces piliers sont, premièrement, une cyberprotection forte et résiliente ; deuxièmement, une gouvernance et des normes efficaces en matière de cybersécurité ; troisièmement, l'édification d'une société sensibilisée à la cybersécurité ; quatrièmement, le renforcement de la protection grâce aux partenariats et à la coopération ; et, cinquièmement, l'élaboration de cadres nationaux.

Pour terminer, je voudrais dire que le Royaume de Bahreïn attend avec intérêt la poursuite de dialogues fructueux sur la cybersécurité à l'ONU, en particulier au Conseil de sécurité, compte tenu de l'évolution rapide des menaces découlant des faits nouveaux liés aux technologies de l'information et des communications.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Pologne.

M. Szczerski (Pologne) (*parle en anglais*) : La diffusion mondiale des technologies numériques, notamment la mise en place et la mise en œuvre du cybergouvernement ou l'administration électronique des ressources liées aux infrastructure critiques, entraîne une dépendance croissante à l'égard du cyberespace. Elle met sérieusement en péril la sécurité et la souveraineté des États. Chaque jour, nous sommes témoins d'un nombre croissant de cyberactivités malveillantes, menées par des acteurs non étatiques et étatiques, qui visent la stabilité et la sécurité des pays et des sociétés.

La Pologne a adopté une position nationale sur l'application du droit international dans le cyberespace en tant que mesure indispensable pour garantir la paix et la sécurité internationales. À cet égard, deux points sont de la plus haute importance pour mon pays. Le premier point, c'est que, dans certaines circonstances, les actions dans le cyberespace peuvent constituer une violation de l'interdiction de l'emploi de la force. Le second point, c'est qu'une cyberattaque peut être qualifiée d'agression armée. Pour nous, le droit de légitime défense s'applique au cyberespace.

L'une des difficultés auxquelles nous sommes souvent confrontés est celui de l'attribution des cyberattaques. En dépit de cela, nous ne cesserons de nous efforcer de traduire en justice les États responsables et les cybercriminels. Il importe d'être conscients que certains États, au lieu de lutter contre les cybercriminels opérant depuis leurs territoires, les préparent et les protègent à des fins politiques ou économiques. Ce faisant, ils compromettent la stabilité et la sécurité des autres. Ils tentent de brouiller les frontières entre les acteurs parrainés par les États et ceux qui sont mus par des motivations criminelles et créent une ambiguïté pour les entités ciblées lorsque celles-ci tentent de se défendre et de demander des comptes aux auteurs de ces actes.

Dans le même temps, un grand nombre d'États ont la volonté politique de mettre en œuvre le droit international et les normes volontaires, mais ne disposent pas toujours des capacités nécessaires pour le faire. Il est dans notre intérêt commun de travailler en étroite collaboration avec eux afin de les aider et de leur proposer un renforcement des capacités adéquat et ciblé. Cela ne se fera pas du jour au lendemain. Par conséquent, nous avons besoin d'une instance permanente pour cette coopération dans le cadre de l'ONU. Dans ce contexte, et conformément à la déclaration faite au nom de l'Union européenne, la Pologne appuie vigoureusement la mise en place du programme d'action. Nous encourageons tous les Membres de l'ONU à l'appuyer et à contribuer activement à sa mise en œuvre opérationnelle.

Les cyberattaques et les activités malveillantes visent à compromettre la paix et la sécurité internationales. Aussi demandons-nous au Conseil de sécurité d'intensifier

ses efforts pour faire cesser et prévenir les activités malveillantes dans le cyberespace. Nous tenons également à appeler un membre du Conseil, la Fédération de Russie, à respecter le droit international et à cesser son agression illégale contre l'Ukraine, non seulement sur le terrain, mais aussi dans le cyberespace et contre ses voisins.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Roumanie.

M. Feruță (Roumanie) (*parle en anglais*) : Je tiens à remercier la République de Corée d'avoir organisé un débat sur un sujet aussi important.

Je voudrais formuler quelques observations en complément de la déclaration faite au nom de l'Union européenne.

Les menaces dans le cyberespace sont persistantes, complexes et destructrices, et elles sont devenues plus fréquentes. La Roumanie est profondément préoccupée par le nombre de cyberactivités malveillantes visant les institutions publiques et les processus démocratiques. Il s'agit d'une menace sérieuse : les cyberopérations, souvent associées à la désinformation, pourraient porter atteinte à l'intégrité des processus démocratiques et à la résilience globale de nos sociétés.

Nous sommes également préoccupés par les cyberattaques contre les infrastructures critiques et les services essentiels, qui pourraient avoir des effets perturbateurs et destructeurs. Nous condamnons avec force les cyberactivités malveillantes qui cherchent à saper nos institutions démocratiques, notre sécurité nationale et notre société libre. Les comportements irresponsables dans le cyberespace créent des risques pour la paix et la sécurité internationales et ne peuvent être tolérés. Le Conseil de sécurité est habilité à traiter ces questions et à encourager une application accrue du principe de responsabilité.

Le droit international s'applique dans le cyberespace. Les États y ont la même obligation d'agir de manière responsable, conformément au droit international, y compris la Charte des Nations Unies, et nous encourageons le Conseil de sécurité à condamner les comportements malveillants dans le cyberespace. Toute utilisation des technologies de l'information et des communications (TIC) par les États d'une manière incompatible avec le droit international et les obligations qui leur incombent en vertu du cadre de comportement responsable des États en matière d'utilisation du numérique, élaboré par l'ONU, porte atteinte à la paix et à la sécurité internationales.

Le renforcement du rôle du Conseil de sécurité dans la lutte contre les cybermenaces, en complément d'autres processus engagés par l'Organisation des Nations Unies concernant les TIC, est à la fois opportun et capital pour le maintien de la paix et de la sécurité internationales dans le cyberespace. Le présent débat public et les précédentes réunions organisées selon la formule Arria en mai 2023 et en avril de cette année confirment l'importante contribution que le Conseil de sécurité peut apporter.

La Roumanie insiste beaucoup sur la nécessité de renforcer la résilience dans le cyberespace. Nous devons améliorer la protection des infrastructures nationales critiques, car des acteurs malveillants tentent de perturber gravement le fonctionnement de nos sociétés. Nous demeurons attachés à l'Initiative internationale de lutte contre les rançongiciels et nous attendons avec impatience qu'elle soit consolidée en tant que riposte internationale coordonnée face à ces menaces. En outre, la nature même du cyberespace appelle à mener un débat prospectif sur le risque que les technologies liées à l'intelligence artificielle n'accroissent l'ampleur et la complexité des cyberattaques, mais aussi sur leur potentiel s'agissant de prévenir et de lutter plus rapidement contre les cyberattaques, et même d'en atténuer les effets.

Pour terminer, nous appelons tous les États à respecter leurs obligations et leurs engagements internationaux en faisant respecter le droit international et en agissant conformément au cadre convenu de comportement responsable des États dans le cyberespace. Nous devons en effet rester fidèles à nos valeurs et principes fondamentaux et agir de manière responsable.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Autriche.

M. Pretterhofer (Autriche) (*parle en anglais*) : L'Autriche souhaite remercier la République de Corée d'avoir organisé le présent débat public qui tombe à point nommé.

L'Autriche s'associe à la déclaration faite au nom de l'Union européenne. Qu'il me soit permis d'ajouter les points suivants à titre national.

Pour répondre aux questions que vous avez posées sur le rôle du Conseil de sécurité, Monsieur le Président, afin d'orienter nos débats, nous pensons que, dans le souci de clarifier les concepts, il convient d'aborder ce débat par le biais du langage commun que nous avons tous adopté : le droit international. Tous les États Membres ont décidé par consensus que le droit international, en particulier la Charte des Nations Unies, s'applique dans son intégralité aux cyberactivités. La Charte est claire : elle confie au Conseil de sécurité la responsabilité de répondre aux menaces qui pèsent sur la paix et la sécurité internationales. Pour s'acquitter de son mandat, il est essentiel que

le Conseil de sécurité continue à faire face aux menaces contemporaines qui pèsent sur la paix et la sécurité internationales. Il est également important de souligner le rôle du Conseil de sécurité dans le règlement pacifique des différends, comme le prévoit le Chapitre VI de la Charte. Les cyberactivités ne se déroulent pas dans un cyberespace virtuel distinct, mais dans le monde réel. Par conséquent, les cyberactivités ne constituent pas un nouveau domaine nécessitant de nouvelles règles ou une application distincte du droit international. En dernière analyse, le Conseil s'intéresse au comportement des États. Il est donc logique qu'il n'hésite pas à se pencher sur une forme de comportement de l'État, à savoir les cyberactivités, chaque fois que cela s'avère nécessaire dans le cadre de son mandat. Par exemple, en ce qui concerne les sanctions, toutes les activités, y compris les cyberactivités, visant à enfreindre les sanctions obligatoires adoptées par le Conseil méritent son attention. À cet égard, il est essentiel d'intégrer la cybersécurité dans les dossiers du Conseil de sécurité.

L'Autriche est attachée à l'état de droit, tant dans le contexte numérique qu'en dehors, et a récemment publié son document de position sur les cyberactivités et le droit international. Elle se félicite de la tenue du présent débat, qui souligne le rôle important du Conseil de sécurité dans l'accomplissement de son mandat, défini par la Charte des Nations Unies, pour faire face aux menaces à la paix et à la sécurité internationales.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Kazakhstan.

M. Umarov (Kazakhstan) (*parle en anglais*) : Je remercie la République de Corée d'avoir organisé la très importante séance d'aujourd'hui.

Le rythme de la numérisation est plus rapide que celui de toute autre innovation dans l'histoire de l'humanité. En l'espace de deux décennies, les technologies numériques ont transformé les sociétés et touché environ 50 % des populations des pays en développement. L'utilisation de la technologie pour améliorer la connectivité et l'accès aux services financiers, commerciaux et gouvernementaux peut réduire considérablement les inégalités démographiques. L'industrie des soins de santé utilise des technologies de pointe qui font appel à l'intelligence artificielle pour sauver des vies, diagnostiquer des maladies et augmenter l'espérance de vie. La disponibilité d'environnements d'apprentissage virtuels et l'apprentissage à distance dans le domaine de l'éducation permettent aux étudiants de participer à des programmes qui étaient auparavant inaccessibles.

Dans le même temps, les technologies de l'information et des communications (TIC) sont utilisées par de nombreux acteurs non étatiques, notamment des groupes criminels et des terroristes, à des fins d'usurpation d'identité, de fraude et de cyberattaque. Elles sont également utilisées pour semer la discorde et diffuser de fausses informations, ce qui peut déstabiliser les États et saper la confiance entre les pays. Les actes malveillants dans le cyberespace peuvent perturber les infrastructures critiques, telles que l'énergie, les transports et les communications, et pourraient donc constituer un multiplicateur de menace dans les conflits existants, ce qui nécessiterait l'intervention du Conseil de sécurité. Cela confirme que les cybermenaces sont en train de devenir un problème géopolitique. À cet égard, le Kazakhstan soutient une approche mondiale responsable de l'utilisation des TIC et de l'intelligence artificielle par l'élaboration de normes généralement acceptées concernant leur utilisation.

Les experts de notre pays participent activement aux travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Nous soutenons le répertoire mondial et intergouvernemental d'interlocuteurs, qui a été lancé en mai. Comme de nombreux États Membres, le Kazakhstan est en train de nommer des interlocuteurs dans les domaines diplomatique et de la technologie qui seront ajoutés au répertoire.

Enfin, je voudrais souligner qu'en période d'instabilité géopolitique, il est important d'éviter de politiser la question à l'examen et de rechercher plutôt un terrain d'entente. Le Conseil de sécurité pourrait jouer un rôle clef dans la coordination des efforts internationaux et la mise en œuvre de mesures spécifiques pour contrer les cybermenaces, notamment en soutenant les initiatives de renforcement des capacités des États, en particulier dans les régions en développement, afin d'améliorer leur capacité à prévenir et à combattre les cyberincidents ; en y associant les acteurs non étatiques, y compris les entreprises du secteur technologique et les organisations de la société civile, afin de renforcer les efforts collectifs de lutte contre les cyberrisques ; et bien sûr, en sensibilisant le public aux questions de cybersécurité et en organisant des examens réguliers des cybermenaces changeantes.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Iran.

M. Iravani (République islamique d'Iran) (*parle en anglais*) : Je vous remercie, Monsieur le Président, d'avoir organisé le présent débat public.

Pour faire face à l'évolution des menaces dans l'environnement des technologies de l'information et des communications (TIC), il convient d'adopter une approche multiforme qui englobe des stratégies technologique, juridique et de coopération.

L'Iran est la principale cible et la principale victime de nombreuses cyberattaques dirigées contre ses infrastructures, attaques qui perturbent fortement la prestation des services publics et le fonctionnement du Gouvernement. Les attaques de Stuxnet et de Duqu contre les installations nucléaires pacifiques de l'Iran en sont des exemples clairs, de même que les cyberattaques contre des infrastructures industrielles critiques, telles que les industries sidérurgique et pétrochimique et les stations-service. Ces activités malveillantes ont mis en évidence le risque de militarisation des TIC pour infliger des dommages aux infrastructures des États.

Compte tenu de la nature complexe de la gouvernance des TIC, je voudrais souligner les points suivants.

Premièrement, il incombe avant tout aux États, à titre individuel, de garantir que les TIC peuvent être utilisées en toute sécurité et en toute confiance. Le rôle prépondérant et la participation active des États dans la gouvernance des TIC au niveau mondial, en particulier dans les domaines politique et décisionnel, doivent être renforcés et garantis. La gouvernance des TIC doit être développée d'une manière qui ne porte pas atteinte au droit des États à définir leur propre développement, leur propre gouvernance et leur propre législation concernant les TIC. Les États doivent agir de manière responsable et conformément aux principes fondamentaux du droit international, en particulier les buts et principes de l'ONU.

Deuxièmement, l'absence de normes universelles juridiquement contraignantes en ce qui concerne les TIC reste problématique. Le droit international actuel est souvent en retard sur le rythme rapide de l'évolution des technologies, ce qui crée des lacunes que les acteurs malveillants exploitent. Il est donc essentiel d'élaborer et d'appliquer des normes internationales juridiquement contraignantes qui tiennent compte des caractéristiques spécifiques des TIC.

Troisièmement, les États doivent s'abstenir d'utiliser les progrès dans le domaine des TIC comme outils pour imposer des mesures coercitives économiques, politiques ou autres, y compris des mesures visant à limiter ou à bloquer d'autres États. Ils doivent également prévenir toute utilisation abusive, y compris par eux-mêmes, des chaînes d'approvisionnement liées aux TIC sous leur contrôle et leur juridiction, en veillant à ce que ces chaînes d'approvisionnement ne développent pas de vulnérabilités qui compromettent la souveraineté et la protection des données d'autres États. Les États doivent prendre des mesures appropriées à l'égard des entreprises et des plateformes dans le domaine des TIC ayant des incidences extraterritoriales qui relèvent de leur juridiction et les tenir pour responsables de leur comportement en ce qui concerne les TIC, en particulier si celui-ci porte atteinte à la souveraineté nationale, à la sécurité ou à l'ordre public d'autres États.

Quatrièmement, nous sommes fermement convaincus que l'environnement des TIC doit être utilisé exclusivement à des fins pacifiques. Dans cette optique, l'ONU doit continuer de jouer un rôle central par l'intermédiaire du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), afin de définir des obligations juridiquement contraignantes visant à empêcher l'utilisation du numérique à des fins malveillantes et à réserver ce domaine à des fins exclusivement pacifiques.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Pakistan.

M. Akram (Pakistan) (*parle en anglais*) : Nous remercions la délégation de la République de Corée d'avoir organisé ce débat important sur l'évolution des menaces dans le cyberespace. Je remercie également le Secrétaire général et les autres intervenants de leurs observations éclairantes.

Les technologies de l'information et des communications (TIC) et leurs applications ont énormément contribué au développement socioéconomique. Toutefois, elles ont également élargi la portée des conflits. La cyberguerre est devenue un nouvel aspect important de la guerre, qui englobe la guerre de l'information et de véritables cyberattaques menées par des acteurs étatiques et non étatiques. Le Pakistan est conscient de la gravité de l'évolution des cybermenaces et de leur incidence sur la paix et la sécurité internationales. Nous reconnaissons également qu'il est urgent de lutter contre d'autres activités malveillantes dans le cyberespace, notamment les rançongiciels et le vol d'informations sensibles.

Plusieurs pays, dont le Pakistan, sont victimes de la désinformation. Dans ses rapports publiés en 2019 et 2020, l'organisation EU DisinfoLab, basée à Bruxelles, a mis au jour la conduite d'activités de propagande et de désinformation anti-pakistanaises et de cyberguerre contre le Pakistan. Le rapport de 2019 apporte la preuve de 15 années d'opérations de grande ampleur contre le Pakistan, impliquant plus de 10 prétendues organisations non gouvernementales frauduleusement accréditées auprès du Conseil des droits de l'homme, plus de 750 faux médias et 550 faux sites Web,

allant même jusqu'à ressusciter des personnes décédées. Il s'agissait d'une campagne systématique menée par un État pour diffuser de fausses informations et instrumentaliser l'ONU, ainsi que des institutions européennes, dans le but de dénigrer le Pakistan. Cette campagne de désinformation, qui a été révélée par EU DisinfoLab, mérite l'attention de la communauté internationale. Nous devons élaborer des modalités permettant d'empêcher cet abus illégal et flagrant des cyberoutils dans le but de promouvoir les discours et les objectifs d'États hostiles.

En décembre 2021, l'Assemblée générale a adopté par consensus la résolution 76/227, intitulée « Combattre la désinformation pour promouvoir et protéger les droits humains et les libertés fondamentales », parrainée par le Pakistan. La résolution affirme qu'il incombe aux États de lutter contre la diffusion de fausses informations qui nuit à la promotion de la paix et de la coopération. En tant que victime d'une cyberpropagande hostile et d'autres formes de propagande, le Pakistan reste déterminé à lutter contre le virus de la désinformation. Nous encouragerons les initiatives dans ce domaine par le biais de la coopération internationale, y compris au sein du Conseil de sécurité.

Tout en reconnaissant le rôle important que joue le Conseil de sécurité dans la lutte contre les cybermenaces spécifiques qui pèsent sur la paix et la sécurité internationales, nous pensons que le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) est le mieux placé pour promouvoir la coopération internationale et des solutions consensuelles aux problèmes que posent les progrès rapides dans le domaine des TIC, et aux possibilités qu'elles offrent.

La Charte des Nations Unies appelle sans équivoque au respect universel des principes de souveraineté, d'intégrité territoriale, de non-recours à la force et de non-ingérence dans les affaires intérieures des États. Ces principes doivent servir de cadre d'orientation pour la cybergouvernance.

Cependant, il ne suffit pas de simplement affirmer que le droit international s'applique au cyberespace. Le Pakistan partage le point de vue selon lequel il est essentiel d'élaborer un instrument international juridiquement contraignant et adapté aux spécificités du numérique afin de fournir un cadre réglementaire et un mécanisme de gouvernance indispensables à la stabilité et à la sécurité du cyberespace. Ce cadre juridique et institutionnel doit tenir compte des préoccupations et des intérêts de toutes les parties, et tous les États doivent participer sur un pied d'égalité aux négociations menées à cet égard au sein de l'ONU.

Des mesures de confiance appropriées, telles que l'échange volontaire d'informations et de bonnes pratiques, peuvent contribuer à accroître la transparence et la prévisibilité dans le cyberespace, tout en réduisant le risque de malentendus et, par conséquent, le risque de conflit. L'inauguration, le mois dernier, du répertoire mondial d'interlocuteurs pour la sécurité numérique constitue une étape importante pour promouvoir la confiance et la coopération entre les États dans ce domaine. Nous devons nous appuyer sur ces mécanismes et cette coopération pour renforcer la cybersécurité et garantir l'utilisation optimale des TIC au profit du développement socioéconomique.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante de l'Uruguay.

M^me^ González (Uruguay) (*parle en espagnol*) : Nous saluons la participation du Secrétaire général ce matin, ainsi que les contributions du Directeur exécutif du CyberPeace Institute et de la professeure de droit et technologie à l'Université Beckett de Leeds et Vice-Présidente du Groupe d'experts en cybersécurité de l'Union africaine.

Nous estimons que l'organisation de ce débat public par la République de Corée, qui préside actuellement le Conseil, arrive à point nommé. Cet exercice met en lumière la question et enrichit le dialogue et les débats sur un sujet qui est capital pour la paix et la sécurité internationales et qui est lié à de nombreuses autres questions relevant de la compétence de l'ONU. L'Uruguay appuie cette initiative ainsi que d'autres types d'initiatives qui cherchent à générer des actions positives face aux répercussions dévastatrices de l'utilisation malveillante des technologies de l'information et des communications (TIC), sous toutes ses formes, sur la paix, la sécurité et la stabilité dans le monde.

Aucune région ni aucun pays n'échappe à ce danger qui ne connaît pas de frontières. La plupart des États Membres ont subi une attaque de cette nature, faisant du cyberespace un lieu peu sûr et aggravant plus encore les fléaux qui frappent nos sociétés, tels que le terrorisme, le trafic de drogue, la traite des personnes et les attaques contre les infrastructures critiques, pour n'en citer que quelques-uns.

Nous avons écouté attentivement l'exposé du Secrétaire général ce matin et nous sommes d'accord pour dire que les dangers liés à l'instrumentalisation des technologies numériques augmentent. Nous condamnons également le recours à l'intelligence artificielle comme multiplicateur de menace dans le cyberespace, ainsi que l'utilisation des technologies quantiques, qui renforcent encore la capacité de nuire.

L'Uruguay est favorable à un usage libre, ouvert et sécurisé du cyberespace qui permet de développer les aspects positifs des technologies et de l'utilisation d'Internet, une approche positive qui nous aidera à atteindre

les objectifs de développement durable, à promouvoir le commerce international et à continuer de faire des progrès scientifiques, médicaux et autres qui contribuent au bien-être de nos populations.

À cette fin, nous devons disposer d'outils concrets et de cadres normatifs sûrs qui garantissent cette sécurité. Cependant, en réalité, tous les pays et toutes les régions ne bénéficient pas des mêmes conditions pour répondre à ces cybermenaces ou pour s'en protéger, en raison de leurs différents niveaux de développement dans les technologies qui comprennent la cybersécurité.

Dans ce contexte, nous sommes préoccupés par l'absence de véritables progrès en matière de renforcement des capacités et de coopération internationale. Plus que jamais, les pays en développement ont besoin du transfert de technologies, de connaissances, de bonnes pratiques et d'équipements nécessaires pour relever efficacement les défis liés à l'utilisation malveillante des TIC.

Face aux difficultés qui se posent dans le cyberespace, l'ONU joue un rôle fondamental pour assurer le maintien de la paix et de la sécurité internationales, qui sont des conditions *sine qua non* pour toute forme de prospérité.

Dans ce contexte, nous soulignons le rôle que joue l'Assemblée générale par l'entremise de la Première Commission. Nous apprécions et soutenons les travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), comme nous l'avons fait par le passé pour les travaux du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale. Leurs travaux ont permis de formuler des recommandations et d'élaborer des normes standardisées sur le comportement responsable des États, créant une base commune de compréhension qui sert de référence, et constituent la principale plateforme de discussion et de débat sur ces questions. Il incombe aux États d'appliquer les normes et les fondements qui en découlent.

Au fur et à mesure que les technologies progressent, les organisations doivent elles aussi être dynamiques. Elles doivent évoluer et améliorer leur cadre institutionnel et leur gouvernance par le biais d'un mécanisme permanent qui leur permette de relever les défis posés par ces mutations. Elles doivent éviter les doubles emplois et, à terme, s'orienter vers l'adoption de règles obligatoires pour tous les États. Le cyberespace n'échappe pas au droit international et aux réglementations internationales, gage de la sécurité juridique.

Nous saisissons cette occasion pour souligner l'importance de la prochaine session du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, également connue sous le nom de Convention sur la cybercriminalité. Nous espérons qu'elle pourra être adoptée le plus rapidement possible et que les États élaboreront des normes nationales en conséquence. Nous pensons que cela permettra à l'Organisation d'avancer dans le traitement positif de cette question.

Enfin, je voudrais réaffirmer l'importance du renforcement de la cyberrésilience et des capacités, qui est un dénominateur commun pour la plupart des Membres de l'Organisation ;les organisations régionales jouent un rôle clef à cet égard. Nous apprécions le soutien des différents pays qui ont mis en place des programmes de coopération et encouragent la formation de techniciens et de professionnels capables de relever les défis liés au cyberespace, et nous les invitons à poursuivre dans cette voie, qui conduira indubitablement à un cyberécosystème plus bénéfique pour tous et toutes, fondé sur la coopération internationale, plutôt que sur l'affrontement ou la politisation de ces questions.

Comme dans d'autres domaines, la synergie entre le Conseil de sécurité et l'Assemblée générale dans la lutte contre les cybermenaces est essentielle. Des séances d'information périodiques et des débats, comme celui-ci, sont nécessaires pour mettre en place des actions efficaces de lutte contre l'utilisation abusive des technologies dans toute la sphère de la sécurité internationale, y compris dans les conflits, et promouvoir ainsi la protection des civils dans les aspects liés au cyberespace.

Je vous remercie, Monsieur le Président, d'avoir inscrit ce point à l'ordre du jour d'aujourd'hui.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante de l'Albanie.

M^me^ Janina (Albanie) (*parle en anglais*) : Dans le monde numérisé d'aujourd'hui, la cybersécurité apparaît comme une question d'importance pour tous les États Membres. Nous tenons à remercier la présidence coréenne d'avoir organisé ce débat important au sein du Conseil de sécurité, ainsi que les intervenants pour leurs contributions utiles.

Beaucoup d'entre nous ont été confrontés à une forme ou une autre de cyberattaque. Nous avons vu ces activités malveillantes non seulement toucher la vie quotidienne de nos citoyens, mais aussi, plus largement,

avoir une incidence sur la communauté internationale dans son ensemble et mettre directement en péril la paix et la sécurité internationales. Le nombre croissant de cyberattaques a un effet considérable sur la réduction du produit intérieur brut des pays dans diverses régions, les pays en développement étant les plus vulnérables.

Les cybermenaces devenant de plus en plus complexes et variées, nos réponses doivent être souples. Nous devons être en mesure d'élaborer de telles réponses et d'atténuer les cybermenaces auxquelles nous sommes confrontés, individuellement et collectivement, en facilitant la coopération internationale et le partage d'informations. Il y a deux ans, l'Albanie a été la cible d'une cyberattaque d'une ampleur sans précédent, menée par plusieurs groupes de pirates informatiques liés à la République islamique d'Iran, dans le but évident de détruire l'infrastructure gouvernementale, de paralyser les services publics et de semer le chaos et l'insécurité dans le pays. Nous continuons à être la cible de cyberattaques sophistiquées.

Dans ce contexte, l'Albanie investit dans sa cyberrésilience nationale, tout en accordant une grande attention aux approches régionales et internationales en matière de cybersécurité. Notre région, les Balkans occidentaux, continue de faire face à un nombre croissant de cybermenaces qui ne cessent d'évoluer. Nous nous efforçons de renforcer les cybercapacités dans la région grâce à des programmes portant sur la cybersécurité, la cybercriminalité et la cyberdiplomatie. Le sommet régional sur la cybersécurité, qui se tiendra en juillet dans mon pays, l'Albanie, visera à renforcer la cyberrésilience dans les Balkans occidentaux.

Nous sommes fermement convaincus que l'on pourrait et devrait faire davantage au niveau international.

Dans ce contexte, je voudrais souligner trois éléments.

Premièrement, le Conseil de sécurité, organe principal chargé du maintien de la paix et de la sécurité internationales, pourrait et devrait se mobiliser davantage. Il s'agit d'une instance précieuse pour discuter des cybermenaces et des moyens d'y faire face. Les discussions doivent être inclusives et ouvertes aux différents acteurs. À cet égard, nous jugeons bénéfique la collaboration entre les gouvernements et le secteur privé pour renforcer la défense contre les cybermenaces.

Deuxièmement, le processus d'application du principe de responsabilité à l'égard des acteurs étatiques et non étatiques malveillants doit être plus présent dans nos efforts conjoints en faveur d'un cyberespace sûr. Cela va de pair avec le respect des normes internationales en matière de comportement responsable dans le cyberespace.

Troisièmement, il est nécessaire de renforcer plus encore les capacités. Alors que les pays développés disposent d'une cyberposture robuste et solide, de nombreux pays en développement manquent de ressources et de compétences spécialisées pour faire face aux cybermenaces. Cela pourrait mettre en péril les infrastructures critiques et rendre vulnérables face à des cyberattaques, au cyberespionnage et à d'autres activités destructrices.

Pour terminer, je tiens à répéter une fois de plus qu'un cyberespace sûr n'est possible qu'en unissant les efforts au niveau mondial, et que la présente séance est un pas dans la bonne direction.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Grèce.

M. Sekeris (Grèce) (*parle en anglais*) : Tout d'abord, je voudrais remercier la République de Corée d'avoir organisé ce débat de haut niveau très important. Mes remerciements vont également nos intervenants pour leurs observations très intéressantes.

La Grèce s'associe pleinement à la déclaration faite par la représentante de la Délégation de l'Union européenne et souhaite faire les remarques suivantes à titre national.

L'évolution numérique de notre époque a été un catalyseur du progrès humain, transformant nos sociétés et nos économies et élargissant les possibilités de coopération. Les technologies émergentes offrent à l'humanité d'importantes possibilités de croissance économique, ainsi que de développement durable et inclusif, touchant les trois piliers de l'action de l'Organisation : la paix et la sécurité, les droits humains et le développement durable.

Alors que nos économies, nos démocraties et nos sociétés dépendent plus que jamais de réseaux et de systèmes d'information sûrs, fiables et de plus en plus interconnectés, la cybersécurité est devenue essentielle à la construction d'un cyberespace mondial, ouvert, libre, stable et sûr.

Dans le même temps, l'exploitation malveillante de ces technologies est devenue une source de nouveaux risques et défis. Les comportements malveillants dans le cyberespace se sont intensifiés ces dernières années, avec notamment une augmentation importante et constante des cyberattaques visant les infrastructures critiques, les chaînes d'approvisionnement et la propriété intellectuelle, ainsi qu'une hausse des attaques par rançongiciels contre les gouvernements, les organisations, les entreprises et les citoyens.

De surcroît, ce qui est encore plus alarmant, les cyberattaques font aujourd'hui partie intégrante des opérations dans le cadre de conflits armés. La Grèce a dit sa vive préoccupation face à ces activités, qui portent atteinte à la paix et à la sécurité internationales et pourraient avoir des effets déstabilisants et en cascade, avec des risques accrus de conflit.

Pourtant, le cyberespace n'est pas un espace de non-droit. Dans le cadre de ce que l'on appelle le comportement responsable des États dans le cyberespace, tous les États ont convenu que le droit international existant, et en particulier la Charte des Nations Unies, était applicable et essentiel au maintien de la paix et de la stabilité. Le droit international doit être respecté et appliqué dans ce domaine de la même manière qu'il s'applique à tous les autres domaines des relations internationales.

Le Conseil de sécurité étant responsable au premier chef du maintien de la paix et de la sécurité internationales, nous espérons qu'il jouera à l'avenir un rôle plus actif dans les questions liées aux menaces émergentes et contemporaines. Ce rôle peut inclure des efforts visant à renforcer le cadre susmentionné de comportement responsable des États et à répondre aux cyberactivités incompatibles avec les objectifs de maintien de la paix, de la stabilité et de la sécurité internationales.

En tant que fervent défenseur de la primauté du droit international et du règlement pacifique des différends, nous réaffirmons notre aspiration à un cyberespace pacifique et sûr, et nous nous engageons pleinement à poursuivre les discussions sur ce sujet très important, y compris pendant notre mandat de membre non permanent du Conseil de sécurité pour la période 2025-2026.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Espagne.

M. Gómez Hernández (Espagne) (*parle en espagnol*) : Nous nous félicitons de la tenue du présent débat public. En tant qu'ardent défenseur et contributeur actif au maintien de la paix et de la sécurité internationales, l'Espagne réaffirme son engagement à lutter contre les cybermenaces et à promouvoir le comportement responsable des États dans le cyberespace par le biais d'une collaboration régionale et internationale dans le cadre de la conduite responsable des États Membres de l'Organisation des Nations Unies.

Si l'évolution rapide de la nature des menaces nous oblige à adapter l'approche et les outils employés pour les contrer de manière conjointe et intégrée, la clef de la cyberrésilience mondiale et nationale reste le recours à des instruments numériques plus nombreux et plus efficaces, qui garantissent la protection des infrastructures critiques dans le monde entier.

Parmi les tendances les plus inquiétantes, citons la prolifération du détournement de données, en particulier contre les infrastructures critiques ; la manipulation de l'information et de la perception par les technologies numériques ; et les attaques contre les chaînes d'approvisionnement internationales, qui exploitent diverses vulnérabilités et entraînent des pertes économiques.

Le concept même de conflit a évolué avec l'apparition de stratégies hybrides, de zones grises et de guerres asymétriques. Une démarcation nette entre guerre et paix en est même parfois caduque. Une utilisation malintentionnée du numérique fait désormais partie intégrante de la gamme complexe et changeante d'outils exploités pour prendre la main dans les conflits. Il est urgent d'adopter une perspective plus large pour aborder les conflits contemporains de manière globale.

Par conséquent, un mécanisme ou engagement international lié au numérique, quel qu'il soit, devra s'appuyer sur les accords convenus autour du cadre de comportement responsable des États dans le cyberespace et résulter d'un processus ouvert, inclusif et transparent.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Portugal.

M. Vinhas (Portugal) (*parle en anglais*) : Je tiens à féliciter la République de Corée d'avoir organisé le débat d'aujourd'hui et je m'associe à la déclaration faite au nom de l'Union européenne ce matin.

Garant de la paix et de la sécurité internationales, le Conseil de sécurité doit être apte à répondre aux menaces tant actuelles qu'émergentes ou futures. Le fait que nous débattons de la question des menaces dans le cyberespace montre que le Conseil sait, lorsque c'est nécessaire, s'adapter aux nouveaux défis.

Les activités et opérations hostiles dans le cyberespace se sont révélées être le défi le plus grave à la prospérité engendrée par la transformation numérique. Elles se sont également révélées être une menace de taille pour l'intégrité de nos institutions et la confiance que leur vouent nos citoyens. Plus inquiétant encore, on ne peut sous-estimer l'incidence qu'a la cyberinsécurité sur le monde physique.

Les cyberacteurs hostiles ont davantage de moyens offensifs, et prévenir leurs attaques et s'en relever coûte de plus en plus cher. Le rôle des groupes cybercriminels, en particulier, a rendu plus complexe le panorama de la

cybermenace. À la suite d'attaques perturbatrices menées par des groupes dits de rançongiciels en 2022, le Portugal a rejoint l'Initiative internationale de lutte contre les rançongiciels. Il convient en outre de souligner que, pour les acteurs parrainés par un État, les rançongiciels servent de plus en plus à couvrir la poursuite d'objectifs stratégiques.

L'intelligence artificielle s'est révélée être un formidable niveleur des capacités de multiples acteurs malveillants, en permettant à des opérateurs peu avancés d'accéder à des possibilités nouvelles, notamment s'agissant de la voilure des attaques. Face à ce panorama des menaces, nous espérons que la future convention des Nations Unies sur la lutte contre la cybercriminalité sera bientôt achevée et qu'elle promouvra une coopération internationale des services répressifs. Une telle coopération contre la cybercriminalité d'acteurs parrainés par un État facilitera l'application du cadre de comportement responsable des États dans le cyberespace, élaboré par l'Organisation des Nations Unies et constitué de lois, normes et mesures de confiance.

Le renforcement des capacités joue également un rôle essentiel, et le Portugal entend lancer, en partenariat avec l'Université des Nations Unies, un programme annuel de renforcement des capacités numériques pour les pays en développement. Le futur mécanisme institutionnel permanent, ou programme d'action, qui doit être appliqué à compter de 2026, devrait également contribuer à réduire la fracture numérique.

Le Conseil peut jouer un rôle important, en complément de celui du groupe de travail à composition non limitée sur la sécurité sur la sécurité du numérique et de son utilisation (2021-2025), qui reste l'instance principale pour approfondir notre compréhension des menaces, des normes et des lois, mais aussi pour promouvoir le renforcement des capacités et de la confiance entre États.

Premièrement, le Conseil pourrait réaffirmer l'éventail des normes de comportement responsable des États qui ont été convenues par consensus au groupe de travail, par exemple en rédigeant une déclaration présidentielle à cet effet. À elle seule, cette mesure reconnaîtrait – c'est important – les effets que les cybermenaces peuvent avoir sur la paix et la sécurité internationales.

Deuxièmement, et pour terminer, le Conseil de sécurité pourrait également tenter d'intégrer, le cas échéant, les préoccupations liées au numérique dans les mandats concernés. Renforcer la résilience des infrastructures critiques face aux cyberactivités hostiles peut, dans certains contextes, contribuer de manière déterminante à améliorer la stabilité à long terme.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante d'El Salvador.

M^me^ González López (El Salvador) (*parle en espagnol*) : Je remercie la République de Corée d'avoir organisé cet important débat sur l'évolution des menaces auxquelles nous sommes confrontés dans le cyberespace.

Comme ma délégation l'a noté à diverses occasions, les menaces associées à l'utilisation du numérique dans le contexte de la sécurité internationale ne cessent d'évoluer en ampleur et en intensité. Combinées à l'utilisation abusive de technologies émergentes telles que l'intelligence artificielle ou l'informatique quantique, ces menaces peuvent engendrer de nouveaux vecteurs d'attaque qui permettent d'exploiter les vulnérabilités des systèmes numériques. La connectivité croissante des infrastructures numériques dans tous les domaines – social, économique et politique – de la gouvernance peut avoir des effets en cascade difficiles à prévoir.

Ainsi, les activités malveillantes dans le domaine du numérique peuvent entraîner des perturbations qui dépassent le cadre international de la paix et de la sécurité. De même, elles peuvent représenter un préjudice direct pour les civils, en particulier lorsque ces attaques sont menées contre des infrastructures critiques nécessaires au fonctionnement de la société, telles que les systèmes de santé publique, les services de base comme l'approvisionnement en eau et en énergie, ou les systèmes de transport, et qu'elles perturbent Internet ou le rendent indisponible.

Mon pays estime que, dans l'exécution de son mandat et de sa responsabilité s'agissant du maintien de la paix et de la sécurité internationales, le Conseil de sécurité devrait aborder, en amont et de manière plus systématique, les menaces à la paix et à la sécurité émanant du cyberespace. Cela pourrait se faire dans le cadre de discussions spécifiques assorties de résultats concrets liés à la protection des infrastructures critiques et des infrastructures d'information critiques, à la détection des incidents de cybersécurité, la riposte qui leur est opposée et leur relèvement en aval, et à une vision transversale du renforcement des capacités en matière de cybersécurité, en particulier pour les pays en voie de développement, entre autres aspects.

En outre, la possibilité d'inscrire à l'ordre du jour thématique du Conseil une question consacrée aux menaces à la paix et la sécurité issues du cyberespace, notamment le numérique et autres technologies émergentes telles que l'intelligence artificielle, pourrait être envisagée, en complément des efforts déployés dans le cadre de l'Assemblée générale et d'autres organes subsidiaires.

Il convient également de souligner la nécessité d'examiner plus avant l'incidence des technologies numériques sur la protection des civils et des biens de caractère civil dans les conflits armés, notamment l'application et le plein respect des principes du droit international humanitaire dans le domaine numérique. Nous estimons que l'intensification de la désinformation, de la diffusion de fausses informations et des discours de haine sur les plateformes numériques, et leurs conséquences, sont des questions qui méritent aussi l'attention du Conseil de sécurité.

En raison de contraintes de temps, la version intégrale de cette déclaration sera disponible au Secrétariat.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante de la Bulgarie.

M^me^ Stoeva (Bulgarie) (*parle en anglais*) : La Bulgarie s'associe à la déclaration faite au nom de l'Union européenne. Je voudrais souligner quelques points à titre national.

Nous félicitons la République de Corée d'avoir organisé le débat de haut niveau d'aujourd'hui et d'avoir porté ce sujet important à l'attention du Conseil de sécurité. Nous tenons à remercier les intervenants de leurs exposés extrêmement éclairants et riches en informations.

La question de l'évolution des menaces dans le cyberespace revêt une importance croissante pour la sécurité et la stabilité de nos sociétés. Aujourd'hui, le cyberespace est de plus en plus exploité à des fins politiques et idéologiques, et la polarisation accrue au niveau international empêche le multilatéralisme d'être pleinement efficace.

Comme l'ont expliqué les intervenants, les campagnes de désinformation appuyées par d'importants moyens qui tentent d'exploiter les vulnérabilités de la société, sapant les processus et les institutions démocratiques, suscitant la méfiance et, en fin de compte, affaiblissant les sociétés sont l'un des plus grands risques auxquels nous sommes confrontés du fait de l'utilisation du cyberespace à des fins malveillantes. En outre, les actions malveillantes visant les infrastructures critiques et les services essentiels constituent également une menace mondiale majeure. Toutes ces activités portent atteinte à la sécurité et à la stabilité internationales, et érodent les avantages que le cyberespace apporte au développement socioéconomique et politique.

Bien que la sécurité nationale, y compris la cybersécurité, demeure une prérogative des gouvernements, les éventuelles répercussions transfrontières des cyberincidents montrent qu'il faut déployer des efforts conjoints. C'est pourquoi il importe de renforcer la coopération sur les questions cybernétiques au niveau international. En outre, alors que de manière générale, le débat multilatéral efficace sur la sécurité internationale dans le cyberespace se détériore en raison des tensions géopolitiques, il est clair que le Conseil de sécurité doit adopter une position plus volontariste sur la question.

La Bulgarie estime que la sécurité et la stabilité internationales dépendent d'un cyberespace mondial, ouvert, sécurisé et stable, où le droit international, en particulier la Charte des Nations Unies, et les normes, règles et principes volontaires et non contraignants de comportement responsable des États sont respectés. À cette fin, la coopération internationale est indispensable. C'est pourquoi il est primordial de renforcer le rôle du Conseil de sécurité dans la lutte contre les cybermenaces. Une participation active 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.

La nature interconnectée du cyberespace requiert que toutes les parties prenantes assument leur responsabilité particulière de maintenir un cyberespace mondial, ouvert, sécurisé et stable et échangent sur la question. Par conséquent, une approche multipartite est vitale pour faire face comme il se doit à l'évolution des menaces dans le cyberespace. Les États et les institutions internationales, y compris le Conseil de sécurité, doivent chercher à renforcer les échanges réguliers et structurés avec toutes les parties prenantes, notamment le secteur privé, le monde universitaire et la société civile. C'est ainsi que l'on pourra également promouvoir et faire progresser la prévention, la préparation, la résilience et la capacité de réaction dans le cyberespace.

Enfin, il convient de noter que le niveau de cyberrésilience et la capacité de détecter les cyberactivités malveillantes et d'y répondre varient considérablement d'un pays à l'autre en fonction de leurs moyens et de la maturité de ceux-ci. C'est pourquoi il faut améliorer le niveau global de cybersécurité en renforçant les capacités et en élaborant des normes communes en matière de cybersécurité, en particulier pour les infrastructures critiques, ainsi qu'en mettant au point de nouvelles technologies et en les appliquant.

Le Président (*parle en anglais*) : Je donne maintenant la parole à M^me^ Andriani.

M^me^ Andriani (*parle en anglais*) : J'ai l'honneur de prendre la parole devant le Conseil de sécurité aujourd'hui pour parler d'une question critique, à savoir l'utilisation abusive des technologies modernes et les menaces croissantes qui pèsent sur le cyberespace.

La cybercriminalité est un multiplicateur de menace, qui favorise d'autres formes de criminalité, aggrave les chocs mondiaux et compromet le développement durable et la paix et la sécurité.

INTERPOL appuie la tenue de ce débat public et propose trois éléments pour renforcer l'architecture de sécurité mondiale face aux cybermenaces que font peser les acteurs criminels non étatiques.

Premièrement, nous devons améliorer notre compréhension du paysage moderne des cybermenaces qui, à ce jour, reste fragmenté entre les régions et les secteurs. À cet égard, INTERPOL a mis au point le projet Gateway pour faciliter l'accès aux données des secteurs, en complément de la mise en commun des informations entre les pays membres. Notre plateforme I-24/7 relie 196 pays membres, permettant un échange sécurisé d'informations policières à l'échelle mondiale. De plus, nous proposons des plateformes de lutte contre la cybercriminalité sur mesure pour l'échange des meilleures pratiques, y compris à des fins d'analyse. En outre, notre liste de points de contact joignables 24 heures sur 24 et sept jours sur sept et nos groupes de travail régionaux facilitent les interventions rapides dans les cas urgents et renforcent la confiance entre les organismes. En travaillant ensemble et en tirant parti des mécanisme d'échange de l'information existants et établis, nous pouvons réaliser des progrès considérables s'agissant de protéger le cyberespace et de garantir la sécurité mondiale.

Deuxièmement, nous devons combler les lacunes en matière de capacités. Des disparités importantes subsistent en matière de cyberrésilience. INTERPOL aide les États Membres à surmonter la fracture numérique en leur fournissant une assistance technique et en renforçant leurs capacités. Nous visons à doter les services de répression des connaissances et des compétences nécessaires pour faire face aux cyberdéfis d'aujourd'hui.

Troisièmement, nous devons exploiter au mieux les synergies grâce à un dialogue institutionnel régulier et à des mécanismes multilatéraux. Rappelons que c'est la collaboration, et non le chevauchement, qui est essentielle. C'est pourquoi INTERPOL participe activement à divers processus cybernétiques au sein et en dehors de l'ONU, notamment le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et le Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

Les cybermenaces ne connaissent pas de frontières, et nos défenses ne doivent pas en connaître non plus. INTERPOL demeure déterminée à faire en sorte que le cyberespace soit plus sûr pour tous grâce à la collaboration, à l'innovation et à un dévouement sans faille.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Inde.

M. Raguttahalli (Inde) (*parle en anglais*) : Je félicite la République de Corée de son accession à la présidence du Conseil de sécurité pour le mois de juin. Je salue l'initiative d'organiser un débat public sur le thème « Faire face à l'évolution des menaces dans le cyberespace ». Je remercie également le Secrétaire général, ainsi que les représentants de la société civile de leurs observations.

Le monde d'aujourd'hui est à l'ère du numérique. La transformation numérique a transcendé toutes les frontières géographiques, politiques et économiques conventionnelles. Avec les progrès rapides et l'adoption de technologies nouvelles et naissantes, telles que l'intelligence artificielle, nos vies sont de plus en plus imbriquées dans l'espace numérique. Dans ce monde interdépendant, des communications personnelles aux infrastructures critiques, la dépendance à l'égard du cyberespace est profonde.

La transformation numérique nous expose également à une myriade de cybermenaces. Les cyberattaques contre les infrastructures critiques, les systèmes d'information et financiers et les réseaux gouvernementaux sont de plus en plus fréquentes et sophistiquées. Le vol de cryptomonnaie, le vol de données, les hypertrucages, la mésinformation et les incitations sont désormais monnaie courante. En outre, il est à noter que l'intelligence artificielle risque d'accroître la portée et l'ampleur des cyberattaques.

L'intégrité et la sécurité des produits numériques, qui constituent les éléments de base du cyberespace, sont compromises. Ces actes sont commis par des acteurs parrainés par les États et par des acteurs non étatiques, ainsi que par des réseaux de criminalité transnationale. Ces activités malfaisantes sapent la confiance dans les chaînes d'approvisionnement mondiales des technologies de l'information et des communications, compromettent la sécurité et créent des points de tension potentiels entre les États. Selon les estimations de la Banque mondiale, les cyberattaques pourraient avoir causé des pertes d'environ 5 200 milliards de dollars dans le monde au cours de la période allant de 2019 à 2023.

Par ailleurs, les terroristes trouvent dans le cyberespace de nouveaux moyens de perpétrer des actes de violence, de radicaliser les jeunes, de procéder à des recrutements, de dispenser des formations et de lever des ressources financières. De nouvelles méthodes qui

prennent la forme d'actifs virtuels et de cryptomonnaies deviennent la norme dans les opérations financières des terroristes. Le terrorisme exploite de nouveaux canaux et de nouvelles méthodes de financement dans le cyberespace, ce qui en fait une question critique pour la sécurité et la prospérité de chaque pays. L'Inde a été victime du terrorisme pendant plusieurs décennies et est consciente de la gravité du cyberterrorisme.

Dans ce contexte, je voudrais souligner quatre points.

Les menaces dans le cyberespace peuvent non seulement mettre en péril la sécurité nationale, mais aussi fragiliser le tissu même de la stabilité et de la coopération mondiales. Aucun pays ni aucune organisation ne peut lutter de façon isolée contre les cybermenaces ; il faut pour cela un front uni.

Il est de plus en plus nécessaire d'établir des instruments internationaux pour faire face aux menaces dans le cyberespace. Le droit international en vigueur n'est pas équipé pour appuyer les ripostes aux cyberattaques. Les cyberattaques contre les infrastructures critiques, les systèmes d'information et financiers et les réseaux gouvernementaux doivent être considérées comme des attaques terroristes. Il faut envisager la possibilité d'appliquer les traités antiterroristes existants au domaine numérique. La communauté internationale doit uniformiser les lois en matière de lutte contre la criminalité terroriste. La coopération mondiale dans ce domaine contribuera à harmoniser les critères de référence, les meilleures pratiques et les réglementations en matière de cybersécurité.

L'Inde participe aux cyberprocessus et aux consultations en la matière qui, sous l'égide de l'ONU, facilitent une participation intergouvernementale mondiale inclusive et transparente dans le but de créer un cyberespace sûr et sécurisé. Nous estimons qu'une collaboration multipartite est essentielle pour s'informer et comprendre les menaces émergentes dans le cyberespace.

Pour terminer, l'Inde est au premier rang des pays qui promeuvent les technologies numériques, la connectivité et la résilience. Elle est attachée à un cyberespace ouvert, sûr, libre, accessible et stable. Elle continuera de collaborer avec la communauté mondiale pour lutter contre les cybermenaces et veiller à ce que la révolution numérique continue à profiter à l'humanité sans compromettre son bien-être collectif et sa stabilité.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Cambodge.

M. Mao (Cambodge) (*parle en anglais*) : Je tiens en premier lieu à vous remercier, Monsieur le Président, d'avoir organisé le présent débat public de haut niveau, qui permet aux États Membres de partager leurs points de vue sur le cyberespace, alors que les cybermenaces deviennent une préoccupation croissante pour tous les pays. Je remercie également S. E. António Guterres, nos intervenants et les orateurs de leurs observations perspicaces.

Il est indéniable que notre monde est aujourd'hui profondément tributaire des technologies numériques. Les progrès rapides des technologies de l'information et des communications ont ouvert d'immenses possibilités, mais ils nous exposent également à des risques nouveaux et changeants qui menacent la paix et la sécurité internationales. L'augmentation récente du nombre de cyberattaques a démontré que les systèmes informatiques sont plus vulnérables que jamais.

À cet égard, le Cambodge s'est engagé à favoriser un environnement numérique sûr pour tous. Nous mettons l'Association des nations de l'Asie du Sud-Est à contribution pour faciliter les programmes de renforcement des capacités et promouvoir l'échange de meilleures pratiques. Nous croyons fermement au pouvoir de la coopération internationale et nous exhortons la communauté mondiale à fournir une assistance technique et à partager ses connaissances afin de renforcer la cybersécurité, en particulier dans les pays en développement.

Au niveau national, le Cambodge a agi avec détermination en créant le Comité pour la sécurité numérique au début de l'année. Ce comité, composé des ministères concernés, dirige nos efforts en matière de cybersécurité, de prévention de la cybercriminalité, de cyberdéfense et de cyberdiplomatie. Cette approche coordonnée nous permet d'évaluer nos besoins, de combler les déficits de compétences et de mettre en œuvre des stratégies efficaces pour protéger nos infrastructures numériques.

Le Cambodge est conscient de l'importance du renforcement des capacités en matière de cybersécurité. Le mois dernier, le Ministre des postes et télécommunications de mon pays a participé activement à la table ronde mondiale sur le renforcement des capacités en matière de sécurité numérique. Nous félicitons le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), présidé par Singapour, des efforts inlassables qu'il déploie afin de promouvoir le dialogue et la coopération au niveau international sur cette question essentielle.

En outre, le Cambodge préconise d'établir des cadres juridiques solides et des normes internationales qui encouragent un comportement responsable dans le cyberespace, défendent la souveraineté nationale et

préviennent les actes malveillants. La collaboration entre les gouvernements, les entreprises et la société civile est essentielle pour partager les informations et mettre au point des solutions innovantes. Nous mettons également l'accent sur les initiatives pédagogiques et de sensibilisation afin de doter nos citoyens des connaissances et des compétences nécessaires pour évoluer en toute sécurité dans le monde numérique.

Pour terminer, le Cambodge est déterminé à travailler avec toutes les nations pour bâtir un avenir numérique sûr et résilient. Nous réaffirmons notre engagement en faveur de la coopération et de la collaboration afin de construire un avenir plus solide, plus sûr et cyberrésilient pour tous. Ma délégation est convaincue qu'ensemble, nous pouvons créer un cyberespace qui favorise l'innovation, la croissance économique et le bien-être de tous nos citoyens.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Brésil.

M. França Danese (Brésil) (*parle en anglais*) : Je remercie la délégation de la République de Corée d'avoir organisé la présente séance.

Comme nous l'avons déclaré lors de la réunion organisée selon la formule Arria en avril par la République de Corée, le Brésil partage avec de nombreuses autres délégations l'inquiétude que suscite l'évolution des menaces en matière de cybersécurité. Nous convenons également de la nécessité d'élaborer des solutions multilatérales afin d'améliorer la cyberrésilience pour tous.

Nous demeurons toutefois convaincus que la meilleure façon d'atteindre cet objectif est de veiller au caractère inclusif de nos discussions, sans faire double emploi. Si nous apprécions les efforts sincères que déploie la République de Corée pour élargir les formats de discussion au sein du Conseil de sécurité, par le biais d'une réunion organisée selon la formule Arria et du présent débat public, nous estimons que l'instance appropriée pour tenir ces débats reste l'Assemblée générale.

Cette année, nous avons constaté les limites de la capacité du Conseil à établir des règles pour de nouveaux domaines lorsqu'à deux reprises, il n'a pu adopter un projet de résolution sur le déploiement d'armes dans l'espace (voir S/PV.9616 et S/PV.9630). À ces deux occasions, les délégations ont fait part de leurs préoccupations s'agissant de porter à l'attention du Conseil des questions complexes qui seraient traitées plus efficacement par l'ensemble des États Membres de l'ONU. Ces préoccupations sont valables et s'appliquent également dans le cas présent.

Le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) est chargé de débattre de cette question précise et a démontré son efficacité s'agissant de détecter les cybermenaces. Il a mis en évidence les menaces liées aux rançongiciels et aux cryptomonnaies, ainsi que d'autres vecteurs d'attaque, notamment contre les infrastructures critiques. Il a débattu des effets de contagion des cyberattaques et des mesures à prendre pour protéger et différencier les systèmes qui revêtent une importance humanitaire particulière. Il a clarifié l'applicabilité du droit international et du droit international humanitaire au cyberespace. Il réfléchit actuellement à des mesures concrètes pour mettre en œuvre le cadre de comportement responsable des États dans le cyberespace. Il s'agit là de résultats importants qui illustrent l'importance d'organiser ces débats dans l'instance appropriée et la viabilité de cette ligne de conduite.

Cela ne signifie pas que le Conseil n'a pas un rôle à jouer. Conformément aux pouvoirs et fonctions que lui confère la Charte des Nations Unies, cet organe peut réagir à des cyberincidents spécifiques et concrets qui constituent une menace pour la paix et la sécurité internationales.

À une époque où les progrès en matière de désarmement sont quasiment au point mort, le domaine de la cybersécurité se distingue par les avancées notables enregistrées à l'Assemblée générale. Nous devons nous efforcer de maintenir cet élan.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante du Guatemala.

M^me^ Rodríguez Mancia (Guatemala) (*parle en espagnol*) : Le Guatemala remercie la République de Corée d'avoir, en sa qualité de Présidente du Conseil de sécurité, organisé cet important débat public.

Ma délégation reconnaît que le cyberespace est devenu un domaine central et indispensable pour l'activité mondiale et qu'en raison de sa nature civile et à double usage, il a été utilisé par des groupes criminels et terroristes à plus d'une occasion. Cela a entraîné une augmentation de l'exploitation des infrastructures critiques et du nombre de cyberattaques les visant, touchant notamment les réseaux électriques, les systèmes de transports, les hôpitaux et les écoles, avec des conséquences dévastatrices sur la vie des gens et sur l'économie. Les réseaux interconnectés à l'échelle mondiale et la numérisation de l'économie mondiale ont ouvert un espace dans lequel les atteintes à la cybersécurité peuvent constituer de graves menaces pour l'économie et la sécurité internationale.

Les activités malveillantes dans le cyberespace peuvent multiplier les conflits de plusieurs manières. Elles peuvent aggraver les tensions entre États en facilitant des attaques secrètes et en offrant la possibilité d'opposer un déni plausible, ce qui complique l'établissement des responsabilités et encourage la méfiance. En outre, les acteurs étatiques et non étatiques peuvent utiliser le cyberespace à des fins de propagande, de désinformation et d'espionnage, créant ainsi des divisions internes et alimentant les conflits internes et transnationaux.

D'autre part, il est indéniable que l'intelligence artificielle recèle un important potentiel de contribuer au progrès de l'humanité, qu'il s'agisse de prévenir et de régler les crises, de proposer des services de santé et d'éducation, ou d'optimiser l'action des gouvernements, de la société civile et de l'ONU dans tous les domaines. Cependant, son utilisation malveillante peut saper la confiance dans les institutions, affaiblir la cohésion sociale et menacer la démocratie. À la lumière de ce qui précède, ma délégation estime qu'il est nécessaire de redoubler d'efforts, d'une part en matière de prévention et d'autre part pour faire face aux menaces existantes et potentielles.

Certaines mesures ont déjà été prises pour intégrer les questions de cybersécurité dans les programmes de travail de l'Organisation. Toutefois, les travaux visant à inscrire efficacement ces questions à l'ordre du jour du Conseil de sécurité doivent être renforcés par des actions énergiques. Il convient, par exemple, de mettre en place un mécanisme de sanctions pour réglementer les comportements dans le cyberespace, d'accroître l'assistance aux États pour renforcer leurs capacités en matière de cybersécurité, et de poursuivre la collaboration avec le secteur privé et la société civile pour élaborer des stratégies solides de contrôle des technologies de l'information et des communications.

Le Conseil de sécurité doit jouer un rôle plus important dans la lutte contre les cybermenaces qui compromettent la paix et la sécurité internationales.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Belgique.

M. Kridelka (Belgique) (*parle en anglais*) : Je voudrais tout d'abord remercier chaleureusement la République de Corée d'avoir organisé cette séance.

J'ai l'honneur de prononcer cette déclaration au nom des pays du Benelux, à savoir le Luxembourg, le Royaume des Pays-Bas et mon pays, la Belgique. Les pays du Benelux s'associent à la déclaration faite au nom de l'Union européenne et nous voudrions souligner quatre points supplémentaires.

Premièrement, en ce qui concerne les menaces, comme indiqué précédemment au Conseil, les pays du Benelux restent vivement préoccupés par l'évolution et l'intensification de la menace liée aux cyberactivités malveillantes. Cette menace continue de prendre de l'ampleur et pourrait être encore exacerbée par les technologies émergentes, notamment l'intelligence artificielle et les progrès de l'informatique quantique. Nous sommes préoccupés par l'augmentation des attaques par rançongiciel, du recours aux rançongiciels en tant que service et des cybermenaces malveillantes contre les infrastructures critiques, y compris les secteurs de la santé et de l'éducation, ainsi que les processus électoraux. Les effets de ces activités et le risque de propagation constituent une menace pour la paix et la sécurité internationales.

Cela m'amène à mon deuxième point. Dans le cadre de la Première Commission de l'Assemblée générale, tous les membres ont adopté par consensus le cadre de comportement responsable des États dans le cyberespace. Ce cadre confirme que le droit international, en particulier la Charte des Nations Unies, s'applique au cyberespace. La mise en œuvre de ce cadre reste essentielle pour faire face aux menaces informatiques qui pèsent ou pourraient peser sur la sécurité internationale. À cet égard, les pays du Benelux soutiennent la mise en place d'un programme d'action. Parmi les autres processus pertinents de l'ONU figure l'élaboration d'une convention pour lutter contre la cybercriminalité.

En outre, et c'est mon troisième point, en vertu du Chapitre VI de la Charte, le Conseil de sécurité joue un rôle clair dans le règlement pacifique des différends, y compris dans le cyberespace, en appelant les parties à régler tout différend susceptible de mettre la paix et la sécurité internationales en péril. Nous, pays du Benelux, sommes d'avis que le Conseil a un rôle important à jouer dans la promotion d'un cyberespace ouvert, libre et sûr. Nous nous félicitons donc de l'attention accrue portée par le Conseil à la cybersécurité, comme en témoigne le nombre croissant de séances consacrées à cette question depuis 2016. Les conflits en cours montrent que le cyberespace fait partie intégrante des menaces plus larges qui pèsent sur la paix et la sécurité internationales. C'est pourquoi les pays du Benelux approuvent également vos suggestions, Monsieur le Président, concernant l'intégration des questions cybernétiques dans les travaux en cours du Conseil.

Enfin, quatrièmement, nous pensons qu'une attention accrue doit être accordée aux victimes de cyberopérations. Bien qu'elles soient souvent perçues sous l'angle de la concurrence géopolitique, les cyberactivités malveillantes ont des effets dévastateurs sur les populations et

portent gravement atteinte à leurs droits humains. Par conséquent, afin de maintenir le bien-être et la dignité humaine au premier plan de nos débats, nous plaidons en faveur d'une approche axée sur les victimes.

N'oublions pas non plus les risques importants en matière de protection, y compris dans le cyberespace, que la transformation numérique fait peser sur les personnes touchées par des crises humanitaires. Le Comité international de la Croix-Rouge, notamment par l'intermédiaire de sa délégation pour le cyberespace, basée au Luxembourg, est en première ligne pour relever certains de ces défis, par exemple en développant et en testant de nouveaux outils pour fournir, de manière neutre, impartiale et indépendante, des services numériques aux populations touchées.

Les pays du Benelux vous remercient à nouveau, Monsieur le Président, d'avoir organisé ce débat et saluent les efforts que vous déployez pour sensibiliser à l'importance des cybermenaces et y remédier.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Norvège.

M. Løvold (Norvège) (*parle en anglais*) : J'ai le plaisir de m'exprimer au nom des pays nordiques : le Danemark, la Finlande, l'Islande, la Suède et mon pays, la Norvège.

Je voudrais tout d'abord remercier la République de Corée d'avoir pris l'initiative d'organiser cette séance opportune. Ce n'est que la deuxième séance officielle que le Conseil de sécurité consacre au thème important de la cybersécurité.

Les cybermenaces ont évolué de manière préoccupante depuis que le Conseil a examiné cette question pour la première fois sous la présidence estonienne en 2021 (voir S/2021/621).

Je voudrais souligner rapidement trois types de menaces.

Premièrement, la menace de cyberactivités malveillantes parrainées par un État persiste, notamment dans le contexte de la guerre d'agression illégale menée par la Russie contre l'Ukraine. Les cybercapacités de la Russie ont été utilisées comme une arme en Ukraine pour tenter de saper la confiance dans les autorités et de détruire des infrastructures critiques. Nous continuons d'accorder de l'importance à la cyberdéfense de l'Ukraine, ainsi qu'à la protection de nos propres sociétés contre les acteurs malveillants. Dans ce contexte, nous tenons à souligner une nouvelle fois que le droit international s'applique également au cyberespace.

Deuxièmement, les frontières entre les acteurs parrainés par un État, non étatiques et criminels sont de plus en plus floues. Parmi les principales sources de préoccupation, citons le nombre croissant d'attaques par rançongiciels et le fait qu'un plus large éventail d'acteurs étatiques et non étatiques ont accès à des outils et techniques cybernétiques sophistiqués.

Troisièmement, enfin, dans le contexte de toutes ces menaces, le fait que des acteurs malveillants prennent de plus en plus pour cible des secteurs et infrastructures critiques est particulièrement préoccupant.

Les pays nordiques souhaitent souligner en particulier l'importance de la collaboration multipartite en matière de cybersécurité pour répondre à ces menaces. Nous devons nous employer à renforcer la coordination entre les gouvernements et toutes les parties prenantes, y compris la société civile, les milieux universitaires et le secteur privé. Grâce à son accès à l'information, le secteur privé occupe une place essentielle dans le cyberespace, car les entreprises de technologie et de cybersécurité jouent un rôle clef dans la prévision et la réponse aux menaces. Il est important de mieux exploiter les connaissances et les capacités des parties prenantes concernées pour favoriser un cyberespace libre, ouvert, pacifique et sûr.

Compte tenu de l'évolution des menaces, les pays nordiques estiment qu'il est de plus en plus pertinent que le Conseil de sécurité débatte plus régulièrement de la cybersécurité. Les débats au sein du Conseil de sécurité sur les cybermenaces actuelles et émergentes, dans le cadre de discussions thématiques ou portant sur certains pays, peuvent contribuer à sensibiliser aux menaces, à mettre en commun les enseignements tirés et à formuler des réponses appropriées.

Les travaux du Conseil complètent également les discussions menées dans d'autres instances. Dans cet esprit, je voudrais terminer en réaffirmant l'appui des pays nordiques à l'instauration d'un programme d'action sur la cybersécurité, qui servira de mécanisme permanent, inclusif et orienté vers l'action pour promouvoir un comportement responsable des États dans le cyberespace.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Croatie.

M. Šimonović (Croatie) (*parle en anglais*) : Je vous remercie, Monsieur le Président, d'avoir organisé ce débat public opportun, et je remercie nos intervenants de leurs contributions.

La Croatie s'associe à la déclaration faite au nom de l'Union européenne, et je voudrais ajouter certains commentaires à titre national.

Nous observons une multiplication de cybermenaces toujours plus sophistiquées. Il s'agit notamment des attaques par rançongiciel visant les infrastructures critiques, des campagnes persistantes et des ingérences étrangères dans les processus démocratiques, pour n'en citer que quelques-unes. Chacune de ces activités est susceptible de déstabiliser des gouvernements, voire la paix et la sécurité en général.

Dans les zones de conflit, les cyberopérations peuvent amplifier les effets d'une guerre conventionnelle, surtout lorsqu'elles visent des infrastructures critiques, en entraînant des hostilités plus intenses et des préjudices civils plus importants. À cet égard, nous félicitons le Comité international de la Croix-Rouge d'avoir souligné que le cyberespace n'est pas un domaine de non-droit, et nous réaffirmons que le droit international humanitaire s'applique autant dans le monde physique que dans le cyberespace.

C'est pourquoi le Conseil de sécurité doit envisager d'approfondir sa compréhension de cette question extrêmement complexe, via des échanges réguliers avec de multiples parties prenantes non seulement du domaine de la cybersécurité, mais aussi de la consolidation de la paix, de la prévention des conflits et de la médiation. Cela peut impliquer des séances d'information et rapports réguliers sur les cybermenaces, qui permettraient au Conseil et aux États Membres d'être tenus au fait des dernières évolutions et tendances.

En outre, le rôle du Conseil de sécurité pour combattre les cybermenaces pourrait se développer en parallèle des travaux lancés par d'autres organismes des Nations Unies et initiatives multilatérales, d'une manière complémentaire et qui les renforce mutuellement. Il s'agit notamment des travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), et d'autres cadres pertinents, en place ou à venir, afin de garantir une approche coordonnée et globale à l'échelle du système. Le Conseil pourrait également examiner comment il contribue à désamorcer les tensions en encourageant le dialogue et les mesures de confiance entre États, ce qui atténuerait le risque que les cyberconflits ne dégénèrent en affrontements armés.

En prenant des mesures en amont pour comprendre et réduire les cybermenaces, promouvoir la coopération internationale et intégrer les considérations numériques dans son mandat plus large, le Conseil pourrait jouer un rôle important dans l'écosystème de cybersécurité en place à l'ONU et mieux préserver la paix et la sécurité internationales à l'ère numérique.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante du Chili.

M^me^ Narváez Ojeda (Chili) (*parle en espagnol*) : Nous sommes heureux de l'occasion qui nous est donnée de participer à ce débat public. Nous prenons note des exposés et contributions de nos intervenants. Nous profitons de l'occasion pour féliciter la République de Corée de sa présidence du Conseil de sécurité pour le mois en cours.

Comme nous l'avons déjà dit à diverses reprises, le Chili considère que les cyberattaques et les activités malveillantes dans le cyberespace sont une menace pour la paix et la sécurité internationales et qu'elles peuvent avoir des incidences diverses sur les États, en fonction de leur niveau de progression numérique, de leurs capacités, de leur sécurité, de leurs infrastructures ou de leur développement. Nous soulignons tout particulièrement que ces menaces peuvent également avoir des incidences différentes sur des groupes et entités différents, comme dans le cas des femmes, des filles, des enfants et des adolescents.

En ce qui concerne les tendances émergentes et mouvantes des activités malveillantes dans le cyberespace, citons le recours à l'intelligence artificielle et à l'apprentissage automatique, l'association de tactiques multiples de vecteurs d'attaque, les attaques par la chaîne d'approvisionnement qui compromettent l'intégrité des produits et des services, ou encore les attaques sur les appareils connectés à l'Internet des objets.

Il convient également de souligner le risque que représentent les logiciels malveillants comme les rançongiciels, les logiciels de type *wiper* ou les chevaux de Troie, et les techniques telles que l'hameçonnage et le déni de service distribué. Ce sont là des menaces qui, entre les mains d'acteurs malveillants, peuvent faire des ravages dans le fonctionnement des pays et nuire tant à leurs économies qu'au bien-être de leurs populations.

C'est pourquoi nous pensons qu'il est fondamental de renforcer le travail commun et la coopération entre les États. Cela comprend l'échange d'expériences et d'enseignements tirés de la pratique, l'application des normes en vigueur en matière de comportement responsable des États dans le cyberespace, le respect du droit international et du droit humanitaire international, les mesures de confiance et le renforcement des capacités, autant d'éléments qui contribuent à atténuer la méfiance entre les États et à favoriser la stabilité dans le cyberespace. Le Chili est favorable aux éléments précités et considère en outre que cet effort doit associer aux débats et discussions pertinents toutes les parties intéressées compétentes, qu'il s'agisse de la société civile, des universités, du secteur privé, ou des milieux techniques.

Nous soulignons qu'il faut renforcer le rôle du Conseil de sécurité face aux menaces qui pèsent sur le cyberespace, et nous estimons qu'il peut apporter une contribution notable à l'instauration d'un cyberespace sûr, ouvert et pacifique, dans l'intérêt de toutes les nations. Le Chili accorde une grande importance à cette question particulière, car les acteurs malveillants exploitent les vulnérabilités des pays qui ne disposent pas des outils ou de la formation nécessaires pour combattre ces menaces.

Dans ce sens, le Conseil pourrait être un outil inestimable pour créer des espaces de dialogue et de coopération en matière de renforcement des capacités et d'assistance technique, lesquels profiteraient aux pays qui en ont le plus besoin. Nous lançons un appel pour que le Conseil relève le défi de l'évolution du panorama des menaces dans le cyberespace, en y associant la coopération internationale, ce qui, selon nous, devrait pouvoir réunir le consensus.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Népal.

M. Thapa (Népal) (*parle en anglais*) : Je remercie la présidence coréenne du Conseil de sécurité d'avoir organisé ce débat public. Par ailleurs, je félicite les intervenants de leurs contributions éclairantes et fort utiles.

Les progrès rapides observés dans le numérique et l'intelligence artificielle ont révolutionné nos vies, générant des possibilités sans précédent d'accélérer le développement social et économique. Notre dépendance à l'égard des technologies ne cesse de croître. Toutefois, leur utilisation abusive fait apparaître des menaces nouvelles et graves. Nous nous inquiétons de l'explosion des cas d'attaques par rançongiciel, de la cybercriminalité, de la diffusion de mésinformation et de la haine partout dans le monde.

Aucune infrastructure, aucun système n'est à l'abri d'une cyberattaque, qu'il s'agisse d'infrastructures civiles telles que les institutions financières, les hôpitaux, les systèmes de transport ou d'approvisionnement en eau et en énergie, ou de systèmes militaires de commandement et de contrôle d'armes nucléaires ou de systèmes d'armes autonomes. Cela compromet la paix, la sécurité, la stabilité et le développement à l'échelle internationale.

Au Népal, nous sommes nous aussi confrontés aux immenses défis que recèle cette menace puisque des institutions bancaires, des sites de l'administration en ligne et des serveurs népalais ont été victimes de diverses cyberattaques et autres attaques par rançongiciel.

Dans ce contexte, je voudrais souligner certains éléments.

Premièrement, nous devons mettre en œuvre un ensemble robuste de règles fondées sur les normes convenues du droit international, y compris la Charte des Nations Unies, tout en garantissant l'ouverture, la stabilité et la sécurité du cyberespace. Nous devons parvenir à une compréhension commune de l'application des règles et promouvoir des mesures de confiance et un comportement responsable des États dans le cyberespace.

Deuxièmement, nous devons régulièrement organiser des séances d'information et procéder à des évaluations intégrant les éclairages des sociétés technologiques, du secteur privé, de la société civile et du monde universitaire. Cela nous permettra de partager nos connaissances et meilleures pratiques et de nous tenir prêts à faire face à l'évolution du panorama des cybermenaces.

Troisièmement, les pays comme le Népal sont plus vulnérables à ces nouvelles menaces. L'absence de cadres juridiques et réglementaires adéquats, les capacités humaines limitées et les ressources financières sont autant de défis que nous devons relever pour nous préparer à prévenir et à contrer ces menaces. Une assistance et un appui internationaux soutenus sont par conséquent essentiels pour renforcer les capacités de pays comme le Népal afin qu'ils puissent prévenir les cyberattaques et y répondre. Nous devons promouvoir les partenariats multipartites afin de combler les lacunes en matière d'institutions, de compétences, de capacités, de technologies et de ressources.

Quatrièmement, nous devons promouvoir la cybersécurité par le biais d'un développement inclusif et d'une prospérité pour tous et toutes en réduisant la fracture numérique entre les États.

Pour terminer, les cybermenaces auxquelles nous sommes confrontés sont importantes. En prenant des mesures volontaristes, globales et coordonnées, nous pouvons garantir un cyberespace sûr, ouvert et pacifique pour tous et toutes. Alors que nous progressons dans la réalisation de notre programme pour un avenir durable et numérique sans exclusive, nous devons construire ensemble une communauté mondiale résiliente, capable de résister aux menaces de l'ère numérique et de les surmonter.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Bangladesh.

M. Muhith (Bangladesh) (*parle en anglais*) : Je remercie la République de Corée, qui préside actuellement le Conseil de sécurité, d'avoir organisé cet important débat public. Je remercie également les intervenants de leurs exposés éclairants.

Dans le paysage numérique en évolution constante, les cybermenaces sont devenues omniprésentes et elles sont souvent imminentes, perturbant les structures financières, démocratiques, socioculturelles et sécuritaires du monde. Le Global Risk Report 2024 (rapport sur les risques mondiaux 2024) souligne que les cybermenaces constituent l'un des défis les plus graves de notre époque, estimant le coût potentiel de la cybercriminalité à 24 000 milliards de dollars d'ici à 2027. Un chiffre aussi stupéfiant exige une action immédiate et urgente de notre part. Mais au-delà du coût en termes économiques, les conséquences effroyables de la cybercriminalité sur les personnes et les sociétés ne sauraient être sous-estimées.

Pour répondre aux questions posées par le Président pour orienter le débat, je voudrais souligner plusieurs points : premièrement, la prolifération des cybermenaces, y compris les attaques par rançongiciels, le cyberespionnage et les campagnes de mésinformation et de désinformation par le biais d'hypertrucages et autres moyens, fait peser des risques importants sur la paix et la stabilité dans le monde. Ces menaces visent les infrastructures critiques et sapent les processus démocratiques et l'harmonie sociale en propageant la xénophobie, l'intolérance et les stéréotypes. En outre, les progrès de l'intelligence artificielle et de l'informatique quantique ont amplifié la portée et la complexité des cybermenaces. Alors que des milliards de personnes dépendent des plateformes numériques pour leurs activités quotidiennes, il est plus urgent que jamais de parer à ces menaces.

Deuxièmement, nous sommes fermement convaincus que, face à des menaces aussi graves, la force du tout dépend du maillon le plus faible. C'est pourquoi l'amélioration de la coopération et de la coordination internationales est indispensable de nos jours. Il est impératif d'affermir les mesures de cybersécurité, d'encourager les mécanismes d'échange d'informations et d'investir dans des initiatives de renforcement des capacités pour améliorer la résilience face aux cybermenaces. À cet égard, nous soulignons l'importance du respect des principes de l'égalité souveraine et du droit international dans le domaine numérique. Nous devons trouver des moyens de concilier la liberté d'expression et la nécessité de lutter contre la diffusion néfaste de mésinformation.

Troisièmement, dans ce cyberpaysage en évolution rapide, nous félicitons le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) d'avoir facilité une collaboration et un débat internationaux essentiels. L'Assemblée générale, qui reflète la volonté et les aspirations globales de la communauté internationale, reste la principale instance pour ces discussions cruciales, permettant à tous les États de participer activement à l'élaboration de notre cyberavenir collectif. Nous espérons également que le pacte numérique mondial, en cours d'élaboration, jouera un rôle essentiel dans le règlement de ce problème, et nous plaidons pour une approche collaborative entre l'Assemblée générale et le Conseil de sécurité en vue de sa mise en œuvre effective.

Enfin, en ce qui concerne la question de savoir si la réponse à l'évolution des menaces dans le cyberespace relève ou non de la compétence du Conseil, puisqu'elle ne fait pas partie du concept traditionnel de sécurité, nous pensons qu'en raison des nouvelles menaces qui pèsent sur la paix et la sécurité, la cybersécurité mérite la plus grande attention de la part de l'ONU. Un dialogue ouvert et transparent doit être mené afin de déterminer quelle serait l'instance appropriée pour traiter cette question cruciale, au lieu d'en faire un nouveau sujet de divergence et de polarisation.

D'ici là, nous pensons que le Conseil pourrait jouer un rôle essentiel dans la promotion des mesures de confiance, notamment par le biais d'un partage d'informations et d'un échange de vues efficaces. Nous devons travailler ensemble, que ce soit sous les auspices du Conseil ou dans toute autre instance appropriée des Nations Unies, y compris le groupe de travail à composition non limitée, pour élaborer des normes, des règles et des règlements qui favorisent un environnement numérique sûr, sécurisé, non discriminatoire et stable pour tous et toutes. Le Bangladesh réaffirme sa volonté de collaborer avec la communauté internationale pour faire face à l'évolution des menaces mondiales en matière de cybersécurité.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Viet Nam.

M. Dang (Viet Nam) (*parle en anglais*) : Les menaces qui pèsent sur le cyberespace n'ont cessé d'évoluer, tant en termes d'ampleur que de complexité, et posent des défis considérables à la paix et à la sécurité internationales. Ces menaces vont des cyberactivités malveillantes, notamment l'espionnage, les attaques visant les infrastructures critiques et les violations de données, à la mésinformation, la désinformation et la guerre cyberpsychologique. Ces activités peuvent présenter des risques importants pour la sécurité nationale, causer des dommages économiques substantiels et saper la confiance du public dans les institutions.

Aucun pays n'est à l'abri de ces menaces. Il ne fait aucun doute que les pays en développement, qui manquent souvent de capacités solides en matière de cybersécurité, sont les plus vulnérables et servent parfois de terrain d'essai pour la cyberguerre des États-nations et pour la cybercriminalité commise par des acteurs non étatiques.

À l'échelle mondiale, étant donné que le cyberespace ne connaît pas de frontières et que la question de l'attribution peut s'avérer difficile, les cyberattaques peuvent déclencher des conflits et exacerber les tensions géopolitiques. Le règlement de ce problème complexe nécessite donc une approche à multiples facettes, dans laquelle l'ONU joue un rôle important.

Premièrement, il est essentiel que les États respectent et mettent en œuvre les normes et règles existantes du droit international applicable, qui constituent un guide complet pour le comportement des États dans le cyberespace.

Dans le même temps, pour promouvoir la paix, la sécurité et la coopération entre les nations dans la sphère numérique, nous devons continuer à renforcer le cadre international qui régit les cyberactivités, notamment en soutenant pleinement les processus en cours dans ce domaine, y compris le pacte numérique mondial et la Convention sur la cybercriminalité.

Deuxièmement, le renforcement des capacités est essentiel pour maintenir un cyberespace ouvert, sûr, stable, résilient et pacifique, en particulier pour ceux dont les cybercapacités sont limitées, afin de prévenir efficacement les cyberactivités malveillantes, de s'y préparer et d'y répondre. Il est fondamental que tous les États partagent l'objectif commun de renforcer les capacités et de réduire l'écart de développement en matière de technologies de l'information et des communications entre les pays et les régions.

Troisièmement, compte tenu de son mandat, le Conseil doit accorder davantage d'attention à cette question et se pencher sur les liens entre les cybermenaces et d'autres questions clefs inscrites à son ordre du jour, telles que la prévention des conflits, la lutte contre le terrorisme et la protection des infrastructures critiques. Il est également impératif que le Conseil favorise la collaboration avec d'autres organismes des Nations Unies, des organisations régionales et le secteur privé, afin d'élaborer une réponse unifiée et globale aux cybermenaces.

Le Gouvernement vietnamien a adopté une approche globale, à l'échelle de la société, pour lutter contre les cybermenaces en promulguant sa loi sur la cybersécurité en 2018. Le Viet Nam réaffirme son soutien à un effort mondial concerté pour établir des cadres et des mécanismes solides visant à faire respecter les principes de souveraineté, de non-ingérence et de comportement responsable dans le cyberespace. Grâce à une coopération et un dialogue constructifs, nous pouvons relever efficacement les défis liés à l'évolution des technologies tout en préservant l'intégrité du cyberespace mondial et de l'écosystème de l'information.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante du Ghana.

M^me^ Oppong-Ntiri (Ghana) (*parle en anglais*) : Je tiens tout d'abord à vous remercier, Monsieur le Président, d'avoir organisé le débat public de ce jour sur un thème aussi important. Nous remercions également les intervenants de leurs éclairages avisés.

Alors qu'il accepte pleinement l'influence toujours plus dominante de la révolution des technologies de l'information et des communications (TIC), le Ghana reste parfaitement conscient des risques que cette révolution fait également peser sur la paix et la sécurité internationales. Plus près de nous, sur le continent africain, nous sommes témoins de l'incidence et des effets modificateurs de la croissance exponentielle des TIC sur un large éventail de défis et de menaces pour la sécurité nationale. Qu'il s'agisse d'hameçonnage et d'usurpation d'identité, du recrutement d'adeptes par des terroristes ou du commerce d'armes légères et de munitions sur le dark Web, les risques pour la sécurité dans le domaine numérique sont constants. Les entreprises privées et les infrastructures publiques critiques ne sont pas épargnées, ce qui fait peser de graves risques sur la paix et la stabilité dans certains cas. Même dans le domaine de la gouvernance démocratique, l'influence positive des TIC sur l'autonomisation des citoyens africains s'agissant de faire avancer les causes politiques qu'ils ont choisies dans le cadre de la liberté de réunion et d'association pâtit beaucoup de leur utilisation abusive pour diffuser des informations fallacieuses, de la désinformation et de la mésinformation, ce qui met gravement en péril l'unité et la cohésion nationales.

Si de solides capacités de cyberdéfense doivent être mises en place pour faire face à ces tendances croissantes, qui réduisent la confiance du public, nous appelons l'attention sur le fait qu'une réponse calibrée est nécessaire afin d'éviter un empiètement excessif de l'État et les actions qui portent atteinte aux droits et à la liberté des citoyens, ce qui peut devenir en soi une source importante de mécontentement et d'instabilité. D'ailleurs, conscients du défi auquel l'Afrique est confrontée, les dirigeants de notre continent ont pris plusieurs mesures pour renforcer ses cyberdéfenses. À la trente-septième session ordinaire de la Conférence des Chefs d'État et de gouvernement de l'Union africaine, organisée cette année, la cybersécurité a occupé le devant de la scène, des décisions clefs ayant été prises pour faire avancer le programme de la Stratégie de transformation numérique pour l'Afrique. Outre

les efforts visant à accélérer la création d'une stratégie continentale de cybersécurité, les dirigeants africains ont adopté une position commune sur l'application du droit international dans le cyberespace. Nous sommes d'accord pour dire que beaucoup reste à faire pour créer un cyberespace digne de confiance et capable de faire face à des menaces en constante évolution. Nous devons tout mettre en œuvre pour combler le fossé numérique par le renforcement des capacités et l'assistance technique.

En réponse à la question concernant le rôle que le Conseil de sécurité peut jouer dans la lutte contre les menaces à la paix et à la sécurité internationales dans le cyberespace, le Ghana voudrait apporter les trois précisions suivantes.

Premièrement, pour exploiter pleinement l'énorme potentiel du cyberespace au service de la croissance et de la prospérité, il faut une action mondiale concertée pour faire face aux risques émergents et créer un cyberespace fiable, sûr et résilient pour tous. Cela souligne l'importance des rapports de consensus du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, qui ne laissent planer aucun doute sur le fait que le droit international et la Charte des Nations Unies sont applicables et essentiels au maintien de la paix, de la sécurité et de la stabilité dans l'environnement numérique.

Deuxièmement, le débat public d'aujourd'hui, l'un des rares à avoir été organisés récemment sur ce sujet, constitue une nouvelle étape importante dans la reconnaissance des dangers croissants que les acteurs malveillants du cyberespace font peser sur la paix et la stabilité mondiales. Les actions du Conseil doivent viser à compléter le rôle de l'Assemblée générale dans l'élaboration et la promotion de normes de comportement responsable dans le cyberespace. Le Conseil pourrait également envisager d'encourager la mise en place d'un cadre juridiquement contraignant pour le domaine numérique afin de réglementer toute action d'entités gouvernementales ou non gouvernementales menaçant la paix et la sécurité internationales. Ce cadre pourrait tirer parti des connaissances spécialisées des principales parties prenantes dans l'espace numérique afin de coordonner les efforts déployés au niveau international pour riposter à la cybercriminalité et attribuer les responsabilités des crimes aux fins de l'application du principe de responsabilité. Un organe subsidiaire consacré à cette question pourrait constituer un point de départ.

Troisièmement, compte tenu des progrès rapides des technologies de l'information et des communications, en particulier de l'intelligence artificielle, et des dangers potentiels de leur utilisation abusive, le Conseil pourrait envisager de créer une question spécifique à inscrire à l'ordre du jour, consacrée à la cybersécurité, avant de l'intégrer, à terme, dans les différents ordres du jour thématiques et géographiques. Une telle approche donnerait au Conseil tout le temps nécessaire pour délibérer sur ses répercussions et appréhender pleinement la question, ce qui lui permettrait d'élaborer des stratégies globales pour préserver la paix et la sécurité mondiales contre les cybermenaces.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante du Panama.

M^me^ Concepción Jaramillo (Panama) (*parle en espagnol*) : À l'ère du numérique, les menaces causées par les cyberactivités malveillantes continuent de croître. Le Panama reconnaît qu'il importe de mettre en place une architecture mondiale de cybersécurité pour lutter efficacement contre l'évolution de ces cybermenaces. Le Conseil de sécurité, parmi d'autres acteurs et dans le cadre de son mandat, peut jouer un rôle fondamental s'agissant de relever ces défis et de renforcer la coopération internationale afin de préserver notre environnement numérique commun. Cet organe a la responsabilité principale du maintien de la paix et de la sécurité internationales, et cette responsabilité est tout aussi essentielle dans le domaine du cyberespace. En participant activement aux efforts en faveur de la cybersécurité et en se tenant informé des menaces émergentes, le Conseil peut contribuer grandement à la création d'un cyberespace sûr et pacifique pour tous les pays. Il est impératif que nous examinions les moyens d'améliorer la capacité du Conseil de répondre aux cyberactivités malveillantes, qui peuvent nuire aux infrastructures critiques, aux civils et aux efforts humanitaires.

Lorsque nous évoluons dans le paysage complexe de ces cybermenaces, il est indispensable de tenir compte des discussions en cours sur l'élaboration d'une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, qui contribuera à compléter la Convention du Conseil de l'Europe sur la cybercriminalité. Même si cette convention et ses protocoles ont été fondamentaux pour faciliter la coopération internationale dans la lutte contre la cybercriminalité, la nature évolutive des cybermenaces exige que nos cadres juridiques soient adaptés et renforcés. En actualisant et en améliorant ces cadres, nous pourrons mieux répondre aux nouveaux défis du cyberespace et garantir une architecture mondiale de cybersécurité plus résiliente.

Compte tenu de la nature transnationale des cybermenaces malveillantes, il est impératif que le Conseil de sécurité travaille en collaboration avec les États Membres, les organisations internationales et d'autres parties prenantes pour relever ces défis multiformes. En encourageant la coopération, en partageant les meilleures pratiques et en promouvant un comportement responsable des États dans le cyberespace, nous pouvons collectivement atténuer les risques et les vulnérabilités associés à ces menaces. Le Panama estime que ces efforts peuvent être encouragés au sein de certains comités du Conseil, tels que le Comité du Conseil de sécurité créé par la résolution 1540 (2004). De manière générale, le Conseil de sécurité peut assumer des rôles et prendre des mesures particulières pour relever les défis en matière de paix et de sécurité internationales découlant du cyberespace, notamment en élaborant des évaluations et des stratégies sur les cybermenaces et en intégrant la cybersécurité dans ses discussions sur des questions spécifiques. Les cybermenaces sont liées à d'autres questions inscrites à l'ordre du jour du Conseil de sécurité, notamment la protection des civils, la paix et la sécurité en période de conflit armé, la lutte contre le terrorisme, ainsi que le thème des femmes et de la paix et de la sécurité. Les évaluations et les stratégies doivent tenir compte des questions de genre et prévoir la participation des femmes à l'élaboration des politiques, en gardant à l'esprit leur vulnérabilité particulière.

Pour intégrer efficacement les préoccupations liées au cyberespace dans ses travaux, le Conseil peut étudier les moyens de renforcer la cyberrésilience, de promouvoir la coopération internationale et de faire face aux cybermenaces de manière globale. En renforçant la coordination et la coopération et en améliorant les capacités en matière de cybersécurité, nous pouvons construire un environnement numérique plus sûr et plus résistant au bénéfice de tous les pays. Le Panama demande instamment au Conseil de sécurité de prendre des mesures énergiques à cet égard et à ses membres de travailler ensemble pour garantir un cyberespace plus sûr et plus pacifique pour les générations actuelles et futures.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Italie.

M. Jovanovic (Italie) (*parle en anglais*) : Je tiens à vous remercier, Monsieur le Président, d'avoir organisé ce débat public qui tombe à point nommé. Alors que nous évoluons dans une ère marquée par des avancées technologiques rapides, la nécessité d'une approche solide et unifiée de la cybersécurité n'a jamais été aussi urgente.

L'Italie s'associe à la déclaration faite au nom de l'Union européenne et voudrait formuler quelques observations supplémentaires à titre national.

L'Italie est préoccupée par le nombre croissant de cyberactivités malveillantes et par le développement des capacités numériques à des fins militaires. Nous sommes fermement résolus à renforcer la coopération entre tous les États Membres dans le domaine des nouvelles technologies numériques. La présidence italienne du Groupe des Sept vise à tirer parti des efforts de la communauté internationale pour promouvoir un cyberespace ouvert, interopérable, sûr, sécurisé, résilient et respectueux des droits humains, régi par les principes et les règles du droit international. L'Italie appelle au respect de la Charte des Nations Unies et des normes internationales existantes afin de préserver la paix et la stabilité et de renforcer notre sécurité commune.

Le Conseil de sécurité, dont la responsabilité première est de maintenir la paix et la sécurité internationales, est particulièrement bien placé pour répondre aux cybermenaces dans l'intérêt de toutes les nations. La mobilisation du Conseil doit en effet compléter les autres processus en cours de l'ONU, tels que la proposition de programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. Les propositions présentées lors des précédentes séances du Conseil de sécurité visent à optimiser les initiatives collectives qui portent sur les incidences des technologies de l'information et des communications (TIC) sur la sécurité mondiale. L'une de ces suggestions consiste à examiner les questions de cybersécurité dans des cas nationaux spécifiques ou dans le cadre de questions thématiques plus larges, telles que les missions de maintien et de consolidation de la paix, la non-prolifération et la lutte contre le terrorisme.

En outre, nous devons renforcer la capacité de l'ONU à lutter contre les utilisations malveillantes des TIC qui mettent en péril la paix et la sécurité internationales. Cela est particulièrement important en ce qui concerne la protection des civils, des infrastructures critiques et des opérations humanitaires. À mesure que nous avançons, nous devons examiner les principales tendances des activités malveillantes, parfois amplifiées par les nouvelles technologies telles que l'intelligence artificielle, ainsi que le risque qu'elles présentent en tant que multiplicatrices de menace dans les conflits existants, et les mesures spécifiques que le Conseil de sécurité et l'ONU dans son ensemble peuvent envisager pour s'attaquer aux problèmes croissants qui se présentent.

Nous sommes tous conscients des effets potentiellement disproportionnés que les cyberactivités malveillantes peuvent avoir sur les segments vulnérables de nos populations. Nous sommes tous exposés au risque de

cyberattaques visant les infrastructures critiques, telles que les soins de santé ou l'énergie, ou les particuliers et les entreprises. Pour empêcher les auteurs de cyberattaques de récolter les fruits de leurs actes répréhensibles, il est essentiel de renforcer les capacités. À cet égard, l'Italie accueillera le 2 juillet une conférence nationale sur l'amélioration de l'écosystème des entités publiques et privées chargées des activités de renforcement des cybercapacités à l'échelle mondiale. Cela permettra de faciliter la mise en œuvre de projets futurs avec une approche inclusive et multipartite.

Attestant de l'engagement de l'Italie en faveur du succès de cette approche, qu'il me soit permis de réaffirmer notre volonté de travailler avec tous les États Membres pour développer et renforcer les compétences, les processus et les ressources nécessaires afin de s'adapter à un cyberespace en évolution rapide et, en fin de compte, pour garantir un avenir plus sûr pour toutes les nations.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant d'Israël.

M. Kalmar (Israël) (*parle en anglais*) : Israël souhaite se joindre aux autres délégations pour féliciter la République de Corée d'avoir organisé et de présider ce débat très opportun et important sur les cybermenaces et voudrait ajouter quelques observations sur les menaces existantes et changeantes que nous observons dans le cyberespace.

Israël est en première ligne face à une vague de cyberagressions sans précédent. Nos adversaires ne se sont pas arrêtés à la guerre conventionnelle et au terrorisme. Ils cherchent à exploiter le domaine numérique pour saper notre sécurité, semer la discorde au sein de notre population et perturber notre mode de vie. Les cyberattaques sont devenues une réalité quotidienne pour Israël. Nos infrastructures critiques, qu'elles soient gouvernementales, financières ou sociétales, font l'objet d'attaques incessantes de la part d'acteurs étatiques et non étatiques. Ces attaques visent à compromettre la sécurité et le bien-être de nos citoyens, à menacer notre stabilité économique et à déstabiliser nos institutions démocratiques. Les menaces auxquelles nous sommes confrontés dans le cyberespace sont réelles et omniprésentes, et elles exigent notre vigilance et notre action collectives.

Comme de nombreuses nations, Israël comprend les profondes répercussions des cybermenaces. Notre expérience nous a appris que ces menaces ne sont pas théoriques. Le samedi 7 octobre 2023, des milliers de terroristes du Hamas ont franchi la frontière sud d'Israël et ont massacré, brûlé, violé et mutilé 1 200 innocents – femmes, hommes, personnes âgées, enfants et bébés. En outre, des milliers d'autres personnes ont été blessées et plus de 240 citoyens innocents ont été enlevés et pris en otage par les terroristes. Depuis le 7 octobre 2023, Israël fait également l'objet de cyberattaques massives et constantes. Ces attaques sont orchestrées par l'Iran, avec le soutien actif et la participation de ses supplétifs, le Hezbollah, le Hamas et d'autres groupes terroristes, qui lancent des cyberattaques massives contre nos infrastructures les plus critiques et les plus sensibles, telles que nos infrastructures énergétiques et d'approvisionnement en eau et nos hôpitaux. L'Iran doit être condamné pour ses violations flagrantes des normes de comportement responsable des États dans le cyberespace et des normes humaines et morales fondamentales. Outre les cyberattaques, nous subissons une campagne d'influence iranienne massive visant à terroriser les citoyens israéliens et à porter atteinte à notre société libre et démocratique, ainsi qu'à accroître les souffrances des victimes de l'attaque sauvage du Hamas et de leurs familles. Les auteurs de ces attaques utilisent le cyberespace comme un outil et un lieu pour mener leurs activités terroristes, et ils tentent d'ébranler les fondements de la société israélienne.

Les communautés israéliennes et juives du monde entier sont confrontées à une vague mondiale d'incitation, de discours de haine et d'antisémitisme, qui est considérablement renforcée par un comportement coordonné et inauthentique sur les médias sociaux. Nous prenons note de l'évolution des efforts déployés par certaines grandes entreprises technologiques et leurs plateformes de médias sociaux pour atténuer la haine et la violence, mais il reste beaucoup à faire. Nous appelons toutes les plateformes de médias sociaux à faire preuve d'une plus grande responsabilité à cet égard. Les discours de haine, quels qu'ils soient, les appels à la destruction et les appels qui impliquent l'anéantissement d'une population ne devraient pas être autorisés à résonner dans le monde entier.

L'utilisation du cyberespace par le Hamas conjugue un large éventail de stratégies et d'objectifs, comme l'a déclaré la coalition internationale de lutte contre l'incitation du Hamas et son financement, créée par le Président Macron, de la France, à la suite des attentats du 7 octobre 2023, lors de la réunion qu'elle a tenue à La Haye le 15 mai. Les agents du Hamas utilisent diverses plateformes en ligne pour radicaliser, endoctriner, inciter à la violence, propager la haine et la désinformation et collecter des fonds, tout cela dans le but déclaré de l'organisation, qui est de détruire l'État d'Israël par la violence et le jihad. La communication du Hamas dans le cyberespace, qui intègre l'utilisation sophistiquée d'icônes et de symboles pour déjouer les systèmes de contrôle du langage

de l'intelligence artificielle, permet à des groupes et des individus de s'identifier à la vision violente du monde du Hamas et de transférer ces idées du cyberespace au monde réel. Ce transfert se manifeste par une augmentation considérable des dons et des montants collectés, qui s'élèvent à des dizaines de millions de dollars versés sur les comptes du Hamas, par la participation massive à des manifestations haineuses et par les attaques à l'arme blanche motivées par la rhétorique anti-israélienne et antisémite diffusée en ligne par le Hamas. La communauté internationale ne s'intéresse pas encore au cyberterrorisme en tant que tel. Les cyberterroristes ont des motivations distinctes et ne sont pas concernés par les normes internationales. Le monde contemporain ne dispose toujours pas des moyens adéquats pour lutter contre le cyberterrorisme.

Toutes les nations éprises de paix devraient envisager de combler cette lacune le plus tôt possible. Ce qui commence au Moyen-Orient reste rarement dans notre région. Dans ce monde interconnecté, aucune nation n'est à l'abri. La récente recrudescence des cyberincidents dans le monde, des attaques de rançongiciels paralysant les infrastructures critiques aux campagnes de désinformation minant la confiance du public, souligne à quel point il est urgent d'assumer notre responsabilité commune. Non seulement ces menaces mettent en péril nos avancées technologiques et touchent nos économies, mais elles menacent également le tissu même de nos institutions démocratiques et la stabilité mondiale. Israël souligne l'importance de la coopération internationale. Aucune nation ne peut affronter ces menaces dans l'isolement. Nous devons renforcer nos partenariats, améliorer les mécanismes d'échange d'informations et exiger de chaque pays qu'il mette en œuvre les normes et les règles de comportement responsable dans le cyberespace. C'est essentiel pour créer un environnement numérique sûr et stable dans lequel l'innovation peut s'épanouir sans crainte d'être exploitée. La communauté internationale doit s'unir pour condamner les cyberagressions et veiller à ce que ceux qui cherchent à porter atteinte à notre sécurité collective par des moyens informatiques en subissent les conséquences.

Pour terminer, nous devons saisir cette occasion pour réaffirmer notre engagement à préserver l'intégrité et la sécurité du cyberespace. Ensemble, par le dialogue, la coopération et une action énergique, nous pouvons atténuer les menaces qui pèsent sur nous et exploiter le potentiel de transformation des technologies numériques au profit de l'humanité tout entière.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Maroc.

M. Hilale (Maroc) : Monsieur le Président, permettez-moi tout d'abord de vous féliciter pour la tenue de ce débat public au Conseil de sécurité sur un domaine qui revêt une importance capitale dans ces temps troubles de notre monde compte tenu de la nature évolutive et complexe des menaces inhérentes au cyberespace. Je salue la participation émérite du Ministre des affaires étrangères de la République de Corée, M. Cho Tae-yul, du Secrétaire général, M. António Guterres, ainsi que des intervenants, que je voudrais remercier pour leurs exposés exhaustifs.

Le Maroc se félicite de son coparrainage, en compagnie de 62 autres pays, de la déclaration conjointe sur l'utilisation des technologies de l'information et des communications (TIC) dans le contexte de la paix et de la sécurité internationales.

Le Maroc a constamment plaidé pour davantage de coopération entre les États Membres dans le domaine du cyberespace et affirme son soutien aux initiatives établies sous l'égide des Nations Unies, visant à établir un cyberespace sûr, sécurisé et résilient, en tant que domaine commun et partagé qui devrait toujours préserver sa nature pacifique, prospère et qui tire pleinement avantage des opportunités qui se présentent grâce à une utilisation responsable des TIC.

Face à un contexte géopolitique aussi complexe et peu prévisible, la communauté internationale est appelée à poser les jalons d'une transition numérique globale, durable et pacifique, qui restera conditionnée par nos efforts collectifs pour promouvoir la confiance mutuelle, la transparence, l'échange de bonnes pratiques, le renforcement des capacités, l'assistance technique à la demande des États parties et en fonction de leurs besoins, la réduction du fossé qui se creuse entre les pays développés et ceux en voie de développement dans le domaine des TIC, et, plus particulièrement, le respect de la souveraineté nationale et de l'intégrité territoriale des États Membres.

Le Royaume du Maroc, sous la conduite éclairée de S. M. le Roi Mohammed VI, a toujours été un fervent défenseur de l'usage responsable des TIC, de la confiance numérique et de la digitalisation, grâce à sa nouvelle stratégie nationale de cybersécurité 2030, qui a pour objectif de consolider les acquis obtenus et de capitaliser sur les réalisations faites depuis 2012, date d'adoption de la Stratégie nationale de cybersécurité, et ce en vue de mieux soutenir et accompagner une transformation digitale en tant que levier crucial pour le développement socioéconomique.

L'approche marocaine en matière de cybersécurité repose également sur la coopération internationale, y compris avec les pays frères et amis arabes et africains, en vue de bénéficier des avantages et des opportunités que représente ce domaine vital, de manière optimale, dans le cadre de la coopération Sud-Sud et tripartite.

Au moment où l'Organisation des Nations Unies met en place de multiples mécanismes et plateformes dédiés à l'examen des menaces cybernétiques et numériques, le Royaume du Maroc estime que le Conseil de sécurité devrait continuer à s'engager de manière plus dynamique et active dans ce domaine sensible, pour s'acquitter des missions qui lui échoient, notamment dans le maintien de la paix et la sécurité internationales dans le domaine cybernétique, eu égard à la nature des menaces cybernétiques qui ne connaissent pas de frontières.

Nous considérons que le Conseil de sécurité pourrait se pencher davantage sur des discussions plus approfondies sur la définition et la priorisation des menaces cybernétiques posant un risque direct et permanent à la paix et la sécurité internationales, notamment en se focalisant sur points suivants : premièrement, les paramètres clefs qui déterminent qu'une menace a atteint un niveau « alerte » permettant son examen au Conseil de sécurité ; deuxièmement, les mesures à entreprendre pour prévenir l'escalade des menaces cybernétiques ; troisièmement, la tenue d'un débat annuel du Conseil de sécurité qui retrace les menaces émergentes dans le cyberespace ; et quatrièmement, la promotion d'une participation plus prononcée des femmes et des jeunes, du secteur privé, de la société civile et des académiciens, afin de permettre au Conseil de sécurité de rester informé des menaces émergentes dans le domaine des TIC et de leurs impacts sur la paix et la sécurité internationales.

Le Maroc souligne que la poursuite des discussions au sein du Conseil de sécurité sur les menaces cybernétiques offrirait à ce dernier l'occasion de jouer son rôle de premier plan dans l'élaboration de réponses orientées vers l'action et l'atténuation des menaces cybernétiques collectives auxquelles les États Membres sont quotidiennement confrontés.

Pour conclure, nous estimons qu'il est temps de maintenir l'élan généré lors de cette dernière décennie au sein de l'Organisation des Nations Unies, afin de préserver notre engagement collectif et constructif en faveur d'un cyberespace sécurisé, sûr et résilient. La cybersécurité et la cybercriminalité n'existent pas de manière isolée, mais elles ont des impacts étendus qui affectent l'ensemble de la communauté internationale de manière disproportionnée.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Liechtenstein.

M. Wenaweser (Liechtenstein) (*parle en anglais*) : Nous remercions la République de Corée d'avoir poursuivi le processus d'examen de la question de la cybersécurité par le Conseil de sécurité lancé par l'Estonie (voir S/2021/621). La mobilisation du Conseil de sécurité sur ce sujet permet de s'assurer que l'état de droit contribue efficacement à relever les défis technologiques modernes, y compris à faire face à l'évolution des menaces dans le cyberespace, ce qui est au cœur du mandat du Conseil.

L'avènement de nouvelles cybertechnologies dans le monde interconnecté d'aujourd'hui offre non seulement des possibilités de coopération internationale sans précédent, mais présente également un risque de cyberactivités malveillantes aux effets potentiellement désastreux. Face à des cyberattaques de plus en plus fréquentes et de plus en plus sophistiquées, notamment dans le cadre de l'agression de la Russie contre l'Ukraine, nous devons adopter une position claire quant à la manière dont le droit international s'applique au cyberespace.

En premier lieu, nous rappelons le large consensus sur l'application du droit international dans le cyberespace, y compris le droit international humanitaire, le droit international des droits humains, le droit pénal international et, bien sûr, la Charte des Nations Unies. Le Comité international de la Croix-Rouge a affirmé que le droit international humanitaire s'appliquait aux cyberopérations en période de conflit armé, soulignant la nécessité de respecter les normes juridiques même dans l'espace numérique. En outre, étant donné que les cyberopérations sont de plus en plus utilisées pour commettre des crimes internationaux, y compris des crimes de guerre et des crimes contre l'humanité, il est indispensable de comprendre leurs implications dans le cadre du système du Statut de Rome de la Cour pénale internationale (CPI). Des évaluations pertinentes confirment que la Cour peut déjà enquêter sur les cyberattaques et en poursuivre les auteurs. C'est tout à fait logique : le droit international humanitaire s'applique aux cyberactivités, et les violations de ce droit qui atteignent le seuil de gravité fixé par la CPI peuvent donc faire l'objet de poursuites. Un Conseil consultatif, réuni par le Liechtenstein en 2020 et 2021, a publié un rapport clarifiant la manière dont chacun des quatre crimes principaux énoncés dans le Statut de Rome, à savoir le crime d'agression, les crimes de guerre, les crimes contre l'humanité et le génocide, s'applique dans le contexte des cyberopérations.

Pour pouvoir faire face efficacement à l'évolution des cybermenaces, il est essentiel que la CPI puisse engager des poursuites dans les affaires de cybercriminalité et de criminalité facilitée par Internet. S'appuyant sur le rapport du Conseil consultatif, le Procureur de la CPI a récemment lancé un processus de consultation multipartite, en collaboration avec Microsoft, afin d'élaborer une politique de la CPI pour lutter contre la criminalité facilitée par Internet. Cela aidera les praticiens du droit international à mieux comprendre les complexités associées aux poursuites pour

ce type de crimes. En outre, le renforcement du dialogue entre la Cour, l'ONU, les gouvernements, le secteur privé et la société civile favorisera l'élaboration de politiques importantes dans le contexte du cyberespace et, à terme, soutiendra le rôle de la Cour en tant qu'élément clef de l'architecture internationale de paix et de sécurité.

Enfin, le Conseil de sécurité a un rôle crucial à jouer dans l'application du principe de responsabilité pour les cyberattaques, puisqu'il a le pouvoir de saisir la CPI pour qu'elle mène des enquêtes sur les situations pertinentes. La relation entre la Cour et le Conseil de sécurité est essentielle pour garantir que la justice n'est pas dépassée par la nature changeante et l'évolution des outils de guerre.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Türkiye.

M. Çetin (Türkiye) (*parle en anglais*) : Nous vous remercions, Monsieur le Président, d'avoir organisé le présent débat public sur l'évolution des menaces dans le cyberespace.

Les technologies de l'information et des communications (TIC) sont devenues un élément incontournable de la société et de l'économie et sont omniprésentes dans le quotidien de chacun.

Aujourd'hui, les compétences des États en matière de développement et d'utilisation des technologies jouent un rôle important dans leur développement et leur croissance. Si les progrès technologiques offrent de nombreuses possibilités, les cybermenaces évoluent et deviennent de plus en plus complexes. Les failles de sécurité dans les systèmes d'information et de communication menacent fréquemment l'économie, l'ordre public et la sécurité nationale. Le terrorisme, l'espionnage numérique, la fraude, la maltraitance et l'exploitation des enfants sur Internet, ainsi que l'utilisation abusive de données personnelles figure parmi les menaces facilitées par les TIC qui constituent un risque pour la paix et la sécurité internationales.

Nous sommes particulièrement alarmés par le nombre croissant de cyberattaques. Des études montrent qu'en 2023, plus de 317 millions de tentatives d'extorsion par rançongiciel et plus de 6 milliards de tentatives d'utilisation de logiciels malveillants ont été recensées à travers le monde. Grâce aux progrès technologiques, il est plus facile de lancer des cyberattaques, et leurs effets néfastes et le fardeau pour les victimes augmentent rapidement. La lutte contre ces attaques et ces menaces nécessite des méthodes et des instruments actualisés, tant dans la pratique que sur le plan législatif.

Compte tenu de la nature transfrontière des cybermenaces, il est essentiel d'accroître la coopération internationale et de renforcer les capacités dans ce domaine. Dans cette optique, la Türkiye participe à l'échange de renseignements sur les cybermenaces et contribue à l'élaboration de politiques et de stratégies de coopération au sein des organisations régionales et internationales.

Dans le contexte du droit international, la Türkiye est partie à la Convention du Conseil de l'Europe sur la cybercriminalité. Nous participons aussi activement aux efforts déployés à l'ONU, notamment par l'intermédiaire du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Nous sommes d'avis qu'il convient également d'aborder la question des infractions liées au terrorisme, lorsqu'elles sont commises au moyen des TIC, dans le cadre d'une future convention.

Se pose par ailleurs la question de l'applicabilité du droit international dans le cyberespace. La Türkiye est l'un des États qui coparrainent le programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, et appuie fermement les résolutions 77/37 et 78/16 de l'Assemblée générale.

Étant donné que le cyberespace ne connaît pas de frontières et que la cybersécurité fait intervenir de nombreuses parties prenantes, la coopération internationale revêt une importance capitale. Les prestataires de services et les entreprises de sécurité doivent coopérer plus efficacement avec les gouvernements et les organisations internationales afin de contribuer à la cybersécurité mondiale. Nous nous félicitons que le Conseil de sécurité mette l'accent sur l'utilisation du cyberespace pour lutter contre les menaces croissantes, et nous sommes déterminés à poursuivre la concertation et le dialogue à cet égard.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Arabie saoudite.

M. Alwasil (Arabie saoudite) (*parle en arabe*) : Je tiens tout d'abord à féliciter S. E. l'Ambassadeur Joonkook Hwang, Représentant permanent de la République de Corée, de l'accession de son pays à la présidence du Conseil de sécurité. Je souhaite à la délégation de la République de Corée plein succès durant son mandat. Je tiens également à remercier S. E. le Secrétaire général António Guterres, le Directeur exécutif du CyberPeace Institute, M. Stéphane Duguin, et la professeure de droit et de technologie, M^me^ Ifeanyi-Ajufo, de leurs exposés. Ils déploient des efforts inlassables, extraordinaires et considérables pour faire face à l'augmentation des cybermenaces et aux dangers qui pèsent sur la cybersécurité.

La nécessité d'un cyberespace sûr et sécurisé, qui favorise la croissance et la prospérité, est plus urgente que jamais. Cela souligne l'importance de renforcer la cybersécurité en tant que priorité publique afin de protéger les intérêts vitaux des États et leur sécurité nationale. Le Royaume d'Arabie saoudite estime qu'il est vital et nécessaire de renforcer la coopération internationale à cet égard et de consolider les efforts internationaux visant à réduire les cybermenaces. Il est temps que la communauté internationale adopte une approche sérieuse et concrète qui contribue à fédérer les efforts internationaux pour faire face aux cybermenaces par l'intermédiaire des commissions et des organes spécialisés de l'ONU compétents en la matière.

Le domaine de la cybersécurité au Royaume d'Arabie saoudite a connu des avancées fulgurantes et accélérées. Sur la base de la Vision de l'Arabie saoudite à l'horizon 2030, ainsi que des éléments sur lesquels elle se fonde et des objectifs qui y sont fixés, le Royaume s'est engagé sur la voie de la transformation pour élaborer un modèle saoudien de cybersécurité fondé sur une gouvernance centralisée et un fonctionnement décentralisé qui relève de la responsabilité d'organes nationaux.

À cet égard, nous avons créé en 2017 l'Autorité nationale de cybersécurité, qui est l'organe responsable de la cybersécurité dans le Royaume et le point de référence national. Le modèle adopté par le Royaume se veut exhaustif et traite de tous les aspects de la cybersécurité, qu'ils touchent à la législation, à la sécurité, à l'économie ou au développement. Les efforts déployés par le Royaume en matière de cybersécurité ont été reconnus au niveau international, notamment dans l'Indice mondial de cybersécurité de l'Union internationale des télécommunications, qui nous a classés au deuxième rang mondial et au premier rang dans le monde arabe, au Moyen-Orient et en Asie. En outre, dans son classement mondial de la compétitivité, l'Institut international pour le développement de la gestion a placé le Royaume d'Arabie saoudite au deuxième rang mondial dans le domaine de la cybersécurité, et ce, pendant deux années consécutives, en 2022 et 2023. En 2024, le Royaume a confirmé son rôle de pionnier mondial en matière de cybersécurité en se classant à la première place de l'annuaire mondial de la compétitivité.

Le Royaume d'Arabie saoudite est convaincu de la nécessité de renforcer la coopération internationale dans le domaine de la cybersécurité. C'est fort de cette conviction qu'il a créé le Forum mondial de la cybersécurité, une plateforme mondiale réunissant des décideurs du monde entier pour débattre des questions stratégiques liées à la cybersécurité. Lors de sa session de l'année dernière, le Forum a réuni plus de 120 États. En outre, le Royaume a créé le Forum international pour la cybersécurité, une organisation basée dans la ville de Riyad, en vue de renforcer la cybersécurité au niveau mondial, de promouvoir la coopération internationale et le développement socioéconomique en la matière, ainsi que de consolider davantage les efforts internationaux dans le domaine de la cybersécurité afin de favoriser la prospérité humaine dans le monde entier.

Le Royaume d'Arabie saoudite contribue au renforcement des capacités d'un certain nombre de pays et d'organisations internationales. Plus de 40 pays et organisations ont participé aux exercices cybernétiques organisés par le Royaume. De plus, nous avons tenu à faire converger les efforts régionaux en vue de renforcer la cybersécurité dans la région. Ces efforts ont abouti à la création d'un comité ministériel spécialisé dans la cybersécurité sous l'égide du Conseil de coopération des États arabes du Golfe, sur la base d'une recommandation du Royaume. Qui plus est, sur proposition du Royaume d'Arabie saoudite, le Conseil ministériel arabe de la cybersécurité a été créé sous les auspices de la Ligue des États arabes. À leur dernier sommet, les dirigeants arabes ont décidé que le Conseil ministériel, son secrétariat et son bureau exécutif seraient basés dans la ville de Riyad.

Pour terminer, le renforcement de la cybersécurité est la responsabilité de tous, et exige que nous coopérions et travaillions en partenariat afin de créer un cyberespace sûr et sécurisé qui favorise la croissance et la prospérité de tous les peuples du monde.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Argentine.

M. Mainero (Argentine) (*parle en espagnol*) : Nous remercions la République de Corée d'avoir organisé ce débat public de haut niveau sur la cybersécurité, une question à laquelle mon pays attache une grande importance.

L'Argentine estime que les principales menaces auxquelles nous sommes confrontés ne sont pas sans lien avec les événements géopolitiques qui se déroulent aux quatre coins du monde, principalement en raison de la dimension mondiale du cyberespace et du caractère transnational des cyberincidents. À cet égard, nous tenons à souligner que dans le cadre de l'identification des menaces existantes ou potentielles et des mesures prises par les États pour les prévenir et les atténuer, en plus des efforts de coopération et de renforcement des capacités, il ne faut pas violer le droit international, notamment le droit international des droits de l'homme et le droit international humanitaire. Ces efforts ne doivent pas non plus porter atteinte aux principes inscrits dans la Charte des Nations Unies, tels que l'intégrité territoriale et la souveraineté des États, la non-ingérence dans leurs affaires intérieures et le règlement pacifique des différends.

Nous pensons que le rôle du Conseil de sécurité et ses efforts dans le domaine de la cybersécurité ne doivent pas faire double emploi avec d'autres travaux, mais plutôt compléter et mettre à profit les efforts de longue date du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, créé en 2004, ainsi que les travaux en cours du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), qui examinera en juillet le projet de troisième rapport d'activité annuel, en vue de son adoption.

En ce qui concerne la proposition d'organiser une séance d'information régulière pour examiner l'évolution du paysage des cybermenaces dans le cadre du mandat et de l'ordre du jour actuels du Conseil, nous estimons qu'il est essentiel d'envisager la possibilité d'inviter, à ces séances d'information, des représentants du Bureau des affaires de désarmement, en sa qualité de secrétariat du Groupe de travail à composition non limitée, ainsi que la présidence du Groupe de travail et des représentants du monde universitaire, de la société civile et du secteur privé.

S'agissant en particulier des nouvelles menaces dans le cyberespace, nous pensons qu'il serait singulièrement utile au Conseil de sécurité que des représentants du secteur privé lui transmettent des rapports ou lui présentent des exposés puisque, dans la plupart des cas, ils détiennent et exploitent des infrastructures critiques. En outre, ils disposent de capacités et de ressources plus importantes pour étudier le fonctionnement des logiciels malveillants, ce qui leur permet de maintenir en permanence à jour leurs listes de menaces.

Nous apprécions également que, dans la note de cadrage (S/2024/446, annexe), la présidence reconnaisse que le renforcement des capacités est un élément indispensable. Nous pensons que le renforcement des capacités est crucial pour combler les lacunes en matière de cybersécurité, lacunes qui ne font aucune distinction entre les États et les touchent tous de la même manière, indépendamment de leur niveau de développement. Les États ayant des capacités moins importantes en matière de cybersécurité deviennent souvent des maillons faibles susceptibles d'être exploités par des acteurs malveillants. Du fait de son interopérabilité intrinsèque, une vulnérabilité où que ce soit dans le cyberespace mondial peut être très lourde de conséquences. Il est donc impératif de coopérer en matière de renforcement des capacités. Ce n'est que via une coopération internationale robuste et soutenue en la matière que nous pourrons garantir un cyberespace véritablement résilient, ouvert, sûr, stable, accessible, pacifique, libre et interopérable pour tous et toutes.

À cet égard, nous soutenons que le renforcement des capacités est intrinsèquement lié à l'application du cadre de comportement responsable des États dans le cyberespace. La mise en œuvre de normes, règles et principes de comportement responsable dans le cyberespace doit être complétée par la promotion de l'innovation, par une assistance technique aux fins du renforcement des capacités et par un transfert de technologies propice à la résilience numérique, conformément au droit international en vigueur et en tenant compte des besoins des pays en développement. Cela contribuera non seulement au bien-être et au développement économique de nos pays, mais aussi à l'application et à l'adoption, sur un pied d'égalité, du cadre cumulatif et évolutif de comportement responsable des États dans le cyberespace et, partant, à la paix et la sécurité internationales.

L'Argentine s'inquiète particulièrement des opérations recourant de plus en plus fréquemment à des logiciels malveillants, à des rançongiciels ou à l'hameçonnage, et de leurs effets sur les infrastructures critiques. L'écosystème des vulnérabilités de ces infrastructures critiques s'est considérablement élargi, ce qui préoccupe aussi bien les États que le secteur privé et la société civile. Nous soulignons qu'il importe de coopérer avec toutes les parties intéressées afin de poursuivre l'analyse des menaces existantes et potentielles pesant sur le cyberespace et de promouvoir des actions à l'échelle mondiale, comme le partage d'expériences. Dans le même temps, nous envisageons avec grand intérêt les possibilités que recèlent le numérique et d'autres technologies émergentes pour le développement de nos sociétés. Nous sommes conscients que les technologies émergentes sont neutres et que le problème réside dans la manière dont elles sont commandées et utilisées. Dans cette optique, nous reconnaissons l'impératif de trouver un juste équilibre entre les cadres mis en place pour réglementer le transfert des technologies de l'information et de la communication, le droit de tous les États d'accéder aux technologies émergentes pour leur bien-être et leur développement socioéconomique, et la nécessité de contribuer à la résilience du cyberespace, dans l'intérêt de tous.

Enfin, en s'appuyant sur les travaux menés par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), par l'Union internationale des télécommunications et par d'autres instances pertinentes, le Conseil de sécurité peut jouer un rôle crucial en matière de cybersécurité. Il est fondamental de veiller à ce que les actions du Conseil soient conformes aux réglementations et recommandations déjà en place. Une coordination multilatérale rendra

plus facile la coopération entre les États et les organisations internationales, favorisant ainsi une approche unifiée de la cybersécurité.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Géorgie.

M. Inashvili (Géorgie) (*parle en anglais*) : La Géorgie s'associe à la déclaration faite au nom de l'Union européenne. Nous souhaitons également, à titre national, ajouter certaines observations.

Avant tout, je remercie la présidence coréenne du Conseil d'avoir organisé le présent débat public. Je sais également gré aux intervenants de leurs exposés éclairants ce matin.

Les avancées survenues récemment dans le cyberespace sont très propices à l'innovation, au progrès économique et au développement. Elles pourraient renforcer la capacité des États Membres de mieux protéger des sociétés ouvertes et pacifiques. Néanmoins, leur exploitation à mauvais escient est également susceptible de générer des menaces. Les menaces sur la cybersécurité évoluent constamment à mesure que la technologie progresse, avec les logiciels malveillants, l'hameçonnage ou les violations de données, entre autres. Face à une crise mondiale imbriquée, le rôle du Conseil de sécurité reste crucial pour remédier aux menaces qui pèsent sur la paix et la sécurité internationales, y compris celles émanant du cyberespace, et les réduire au minimum.

Depuis quelques années, la communauté internationale constate que certains acteurs, étatiques et non étatiques, peuvent menacer l'ordre international fondé sur des règles en associant des moyens de guerre classique à des méthodes non conventionnelles récemment mises au point. Certains ont recours à des tactiques numériques pour obtenir des avantages stratégiques, comme en mettant hors service des réseaux de communication, en prenant des infrastructures critiques pour cible, ou en compromettant les systèmes militaires.

Dans ce contexte, la Géorgie reste déterminée à promouvoir un comportement responsable des États dans le cyberespace. Notre position en matière de cybersécurité est conforme au cadre normatif élaboré par le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

Ces dernières années, nous observons une plus grande contribution des femmes à la paix et la sécurité. La mobilisation accrue des femmes dans le domaine de la cybersécurité a ouvert la voie à des perspectives plus inclusives et plus variées. Toutefois, malgré les efforts déployés par le Gouvernement géorgien pour garantir un comportement responsable dans le cyberespace, nous voyons tous que la Russie fait un recours agressif à sa panoplie d'outils hybrides contre la souveraineté de la Géorgie. C'est en Géorgie que, pour la première fois, de nombreuses cyberattaques ont été menées en parallèle d'un engagement militaire classique, dans le cadre de l'agression militaire de grande échelle livrée par la Russie en 2008.

Nous considérons donc le renforcement des capacités comme un élément indispensable de la coopération multilatérale. En plus de renforcer les capacités nationales en matière de cybersécurité, il favorise une coopération internationale plus efficace pour remédier aux cybermenaces complexes, qui dépassent souvent les frontières nationales et exigent une riposte coordonnée. Face à une répartition inégale des capacités numériques, nous sommes convaincus que l'ONU peut mieux accompagner les efforts nationaux visant à établir un cadre normatif et aider les États Membres à renforcer leurs capacités afin de combler les écarts existants.

Pour terminer, nous réaffirmons notre volonté de renforcer la cybersécurité au niveau tant national qu'international, tout en soulignant la nature transversale des cybermenaces et la nécessité d'y répondre efficacement par des mesures collectives.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Australie.

M. Larsen (Australie) (*parle en anglais*) : Je remercie vivement la République de Corée de nous avoir réunis pour débattre de cette importante question.

Je suis heureux de prendre la parole au nom du Canada, de la Nouvelle-Zélande et de l'Australie.

Les cybermenaces hypothèquent les possibilités de transformation offertes par les technologies numériques. Ces menaces gagnent en ampleur et en sophistication et sont tout particulièrement problématiques lorsqu'elles sont utilisées dans le cadre de conflits armés. Nous, citoyens et consommateurs, dépendons tous au quotidien de services numériques, aussi les cyberattaques menées contre les infrastructures critiques peuvent-elles avoir des effets dévastateurs et en cascade sur l'ensemble de la société. Elles ont un effet multiplicateur sur les risques en place et peuvent, de la manière la plus fondamentale, menacer le fonctionnement efficace des gouvernements et la confiance qu'ils suscitent auprès du public.

Nous avons vu dans le monde entier des cyberattaques d'ampleur mettre hors service des infrastructures critiques et perturber des services essentiels et

des activités gouvernementales. Nos propres pays en ont fait l'expérience directe. En Australie, une attaque par rançongiciel sur le secteur de la santé a révélé les informations personnelles de millions de personnes. Au Canada, un rançongiciel a paralysé les systèmes de prestataires de soins de santé dans diverses provinces, ce qui s'est traduit par d'importants retards et a mis en péril des informations sensibles relatives à des milliers d'agents de santé et de patients. En Nouvelle-Zélande, la part des cyberactivités répondant à des motivations financières dépasse pour la première fois celle des activités parrainées par l'État.

Dans les situations de conflit armé en cours, nous avons vu des cyberopérateurs militaires déployer des logiciels malveillants aux effets destructeurs contre les réseaux gouvernementaux et privés, et compromettre les infrastructures civiles critiques et les services d'intervention de crise, y compris les services d'urgence et les réseaux d'électricité, de transports et de communication. Nous constatons également un lien clair entre l'utilisation d'outils de rançongiciel pour perpétrer des crimes financiers, y compris le vol de cryptomonnaie, afin de financer directement des programmes d'armes nucléaires et d'armes de destruction massive et l'affaiblissement de nos efforts en faveur de la stabilité mondiale et du désarmement. Le Conseil de sécurité a un rôle crucial à jouer pour empêcher que cela ne se produise. Nous nous félicitons des occasions telles que celle-ci qui nous permettent de discuter des cybermenaces, contribuant ainsi à intégrer ces questions dans les délibérations du Conseil de sécurité et à les faire mieux connaître grâce à la mobilisation des compétences spécialisées de la communauté des parties prenantes, y compris celles des organisations de la société civile.

Nous avons collectivement envoyé un message sans ambiguïté : les activités de tous les États dans le cyberespace ont des limites et sont soumises à des obligations, tout comme elles le sont dans le monde physique. Tous les Membres de l'ONU ont convenu, par consensus, que le droit international existant, en particulier la Charte des Nations Unies dans son intégralité, s'applique au cyberespace. Les États doivent s'engager sans équivoque à agir conformément au droit international et aux attentes définies par les normes non contraignantes convenues.

Pour terminer, nous avons deux demandes essentielles.

Premièrement, nous demandons au Conseil de sécurité d'affirmer le cadre convenu de comportement responsable des États qui sous-tend la paix et la stabilité et promeut un cyberespace ouvert, sûr, stable, accessible et pacifique. La réalisation de ces objectifs fondamentaux nécessite la mise en œuvre et le respect des engagements connexes, soutenus par un renforcement coordonné des capacités afin que tous les États soient mieux à même de relever les défis posés.

Deuxièmement, nous demandons également au Conseil de sécurité d'affirmer que le droit international humanitaire s'applique au cyberespace dans les situations de conflit armé. De telles affirmations renforcent notre engagement collectif à protéger les infrastructures critiques et à promouvoir le droit international, en particulier la Charte des Nations Unies.

Le Président (*parle en anglais*) : Je donne maintenant la parole à M^me^ Courtois.

M^me^ Courtois (*parle en anglais*) : Le Comité international de la Croix-Rouge (CICR) partage les préoccupations de la République de Corée quant au coût humain potentiel des cyberopérations en période de conflit armé.

Le CICR s'emploie à protéger les populations et à leur venir en aide dans plus de 120 conflits armés dans le monde. Dans un nombre croissant de ces conflits, les cyberopérations créent des risques supplémentaires pour leur sécurité et leur bien-être. Trois tendances sont particulièrement préoccupantes.

Premièrement, les cyberopérations perturbent la fourniture de services essentiels aux populations civiles, tels que l'électricité, l'eau et les soins médicaux. Elles mettent en danger des populations qui souffrent déjà de la dévastation et de l'insécurité causées par les conflits armés, et sont souvent menées au mépris du droit international humanitaire.

Deuxièmement, nous sommes profondément préoccupés par l'implication croissante d'acteurs civils – individus, groupes de pirates informatiques et entreprises technologiques – dans des cyberopérations liées à des conflits armés. Plus les civils et les biens de caractère civil sont proches des hostilités, plus ils risquent d'être touchés.

Troisièmement, le CICR et le Mouvement international de la Croix-Rouge et du Croissant-Rouge dans son ensemble, en tant qu'organisations humanitaires, sont également confrontés à la menace croissante que font peser les cyberopérations, notamment des violations de données et des opérations d'information préjudiciables. Si nos opérations de secours sont perturbées ou si la confiance dans celles-ci et notre travail est ébranlée, notre capacité d'aider et de protéger les populations s'en trouvera affaiblie.

Les membres du Conseil de sécurité ont la responsabilité principale du maintien de la paix et de la sécurité internationales, et un rôle clef à jouer dans la protection des populations civiles pendant les conflits armés. Le

Conseil de sécurité a toujours été clair : les guerres ont des limites. Il n'a laissé aucun doute quant au fait que les belligérants ne doivent pas prendre pour cible les civils ou les biens de caractère civil, et que les installations médicales ainsi que les opérations et le personnel d'aide humanitaire doivent être respectés et protégés. Aussi le CICR encourage-t-il le Conseil de sécurité à intégrer dans ses travaux le coût humain potentiel des cyberopérations et à faire systématiquement respecter les limites que le droit international humanitaire impose de longue date à tous les moyens et méthodes de guerre, qu'ils soient anciens ou nouveaux, cybernétiques ou cinétiques.

La résolution 2730 (2024) récemment adoptée, dans laquelle le Conseil de sécurité exprime expressément son inquiétude face aux activités malveillantes liées aux technologies de l'information et des communications (TIC) ciblant les organisations humanitaires et condamne la désinformation et l'incitation à la violence contre le personnel humanitaire, a constitué une première étape importante dans ce sens. Dans le monde numérisé d'aujourd'hui, le Conseil de sécurité ne doit pas négliger les menaces que les activités liées aux TIC font peser sur les populations civiles en temps de conflit armé.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de Kiribati.

M. Tito (Kiribati) (*parle en anglais*) : Kiribati se félicite de l'occasion qui lui est donnée de partager ses réflexions sur l'utilisation des technologies de l'information et de la communication (TIC) dans le contexte de la paix et de la sécurité internationales. Nous tenons à remercier le Secrétaire général et les intervenants s'exprimant au nom d'une organisation non gouvernementale et du monde universitaire de nous avoir fait part de leurs points de vue.

En début de semaine, Kiribati a approuvé la déclaration commune sur cette question publiée par la République de Corée. Nous tenons à la féliciter de son rôle de chef de file en la matière et à saluer la présence du Ministre des affaires étrangères de la République de Corée, M. Cho Tae-yul, qui préside cette séance. Je vous remercie, Monsieur le Ministre, d'avoir souligné le rôle du Conseil de sécurité, qui doit veiller à ce que les TIC soient utilisées de manière responsable pour promouvoir la paix et la sécurité dans le monde et non à des fins qui mettent en péril la paix et la sécurité internationales, en particulier en cette période où les guerres régionales et les conflits violents se multiplient.

Nous partageons les mêmes préoccupations quant à l'utilisation de cyberactivités malveillantes ciblant les infrastructures civiles et aux conséquences qu'elles peuvent avoir sur la vie et le bien-être des personnes, en particulier les membres les plus marginalisés et les plus vulnérables de nos sociétés. Nous souhaitons exprimer notre profonde inquiétude quant aux cyberopérations visant les infrastructures civiles critiques, telles que l'eau et l'électricité. Ces biens sont protégés par le droit international humanitaire. En outre, en vertu du droit international humanitaire, les installations médicales doivent être respectées et protégées. Il en va de même des opérations d'aide humanitaire en période de conflit armé.

Lorsque les parties prenantes expriment leur point de vue sur les cyberopérations préjudiciables dans les situations de conflit armé et appellent à l'application du droit international humanitaire et à des débats sur cette question, elles le font en toute honnêteté, soucieuses de la sécurité de leur population. Imaginons un monde où ces protections ne s'appliqueraient pas aux cyberopérations et demandons-nous si c'est le monde dans lequel nous voudrions vivre et considérer comme notre foyer. Pour nous, la réponse est non, surtout dans le Pacifique où nous jouissons d'une grande paix et d'une grande harmonie avec la nature et avec nous-mêmes.

Nous devons faire respecter le droit international humanitaire dans le cyberespace. C'est pourquoi nous sommes convaincus que la communauté internationale, en particulier le Conseil de sécurité, doit écouter les parties prenantes et les acteurs des organisations non gouvernementales et du monde universitaire qui expriment leurs préoccupations concernant les activités malveillantes des cybercriminels. Nous devons être prêts à défendre et à appliquer les principes du droit international humanitaire. Par conséquent, nous encourageons vivement le Conseil de sécurité à intégrer à se travaux les préoccupations humanitaires découlant des cyberopérations et à faire respecter les limites imposées à tous les moyens de guerre, y compris les cyberopérations, en vertu du droit international humanitaire. Nous ne pouvons pas risquer l'érosion du droit international humanitaire dans le domaine cybernétique émergent lié aux TIC.

Je voudrais conclure en rappelant la déclaration que l'ancien Président des États-Unis Harry Truman a faite il y a 79 ans pour saluer la Charte des Nations Unies qui venait d'être adoptée.

> « Ce n'est que si nous comprenons ce qu'est la Charte et ce qu'elle peut signifier pour la paix dans le monde que le document deviendra une réalité humaine vivante ».

Respectons tous la Charte des Nations Unies dans son intégralité et appelons toutes les entreprises technologiques mondiales, qui contrôlent les TIC et dont la plupart échappent à la régulation des gouvernements, à veiller

à ce que ces technologies soient utilisées de manière responsable pour promouvoir le plein respect de la Charte et pour faire avancer le noble objectif visé par la Charte, à savoir construire un monde plus pacifique, plus prospère, plus humain et plus aimant pour tous et toutes.

Le Président (*parle en anglais*) : Le représentant de la République islamique d'Iran a demandé la parole pour faire une nouvelle déclaration.

M. Ahmadi (Iran) (*parle en anglais*) : Je suis conscient que la séance d'aujourd'hui a été longue et je ne souhaite pas accaparer l'attention des membres du Conseil. Cependant, j'ai demandé la parole pour faire une nouvelle déclaration parce que la représentante de l'Albanie et le représentant du régime israélien ont abusé de cette enceinte pour faire des allégations non fondées contre l'Iran, accusant à tort mon pays de soutenir des cyberattaques.

Nous rejetons et dénonçons catégoriquement ces affirmations sans fondement. En ce qui concerne l'allusion injustifiée à l'Iran faite par la représentante de l'Albanie dans sa déclaration, nous avons répondu à cette fausse affirmation et l'avons rejetée dans la lettre datée du 10 septembre 2022 que nous avons adressée au Conseil de sécurité (S/2022/685). Nous pensons que le Gouvernement albanais a été induit en erreur par des informations erronées émanant d'une organisation terroriste, à savoir l'Organisation Mojahedin-e Khalq, et a attribué à tort cette cyberattaque à l'Iran.

L'Organisation Mojahedin-e Khalq, actuellement située en Albanie, a déjà mené plusieurs attaques cyberterroristes contre des infrastructures critiques de l'Iran, avec l'aide et le soutien de certains États, dont le régime israélien. Cette organisation terroriste a martyrisé de nombreux responsables et civils iraniens par des attentats à la bombe et des assassinats et, depuis 1981, a ôté la vie à près de 17 000 citoyens iraniens.

Malgré cela, le Gouvernement de la République islamique d'Iran a proposé de bonne foi au Gouvernement albanais de coopérer et de collaborer de manière constructive pour clarifier les accusations infondées portées contre l'Iran. Malheureusement, notre demande est restée sans réponse.

Quant aux allégations infondées du régime israélien, nous les rejetons catégoriquement. Il est paradoxal qu'un représentant d'un régime connu pour ses activités malveillantes, criminelles et terroristes, tant dans le cyberespace que dans le monde physique, accuse d'autres personnes de commettre les actes mêmes que le régime israélien a commis à plusieurs reprises.

Depuis plus de neuf mois, Israël, le régime d'occupation, mène une guerre génocidaire et une agression militaire contre le peuple palestinien sans défense et est impliqué dans des actes barbares et terroristes dans la région, en violation flagrante de tous les règles, principes et normes juridiques internationaux, y compris le droit international humanitaire et le droit international des droits de l'homme. Le régime utilise sans vergogne tous les moyens possibles pour décimer cette population vulnérable, notamment en utilisant la famine comme méthode de guerre, en prenant pour cible et sans discrimination des civils, y compris les femmes et les enfants, en menant des attaques délibérées contre des infrastructures civiles vitales et en entravant la fourniture de l'aide et des services humanitaires essentiels aux civils, en violation directe des résolutions pertinentes du Conseil de sécurité.

En outre, ce régime terroriste est depuis longtemps tristement célèbre pour ses cyberattaques contre les infrastructures critiques d'États souverains. Comme cela est indiqué dans la déclaration qui a été prononcée dans cette salle au nom de l'Iran, les attaques de Stuxnet et celles perpétrées par Duqu contre les installations nucléaires pacifiques de l'Iran sont des exemples clairs des activités criminelles et des cyberattaques d'Israël contre des infrastructures critiques. Ce régime a revendiqué ouvertement ces actes criminels, qui démontrent son implication dans des cyberopérations malveillantes.

Compte tenu de ses antécédents de violations flagrantes des principes fondamentaux du droit international, le régime israélien est très mal placé pour accuser les autres ou leur faire la leçon sur le respect de ces principes. Ce régime ne doit pas rester impuni, et le Conseil de sécurité doit veiller à ce qu'il réponde de tous les crimes internationaux qu'il a commis et continue de commettre.

La séance est levée à 17 h 55.