Nations Unies S/PV.9662

Conseil de sécurité

Soixante-dix-neuvième année

Provisoire

9662e séance
Jeudi 20 juin 2024, à 10 heures
New York

Présidents :	M. Cho Tae-yul/M. Hwang	(République de Corée)
Membres :	Algérie	M. Bendjama
	Chine	M. Fu Cong
	Équateur	M. De La Gasca
	États-Unis d'Amérique	Mme Thomas-Greenfield
	Fédération de Russie	M. Nebenzia
	France	M. de Rivière
	Guyana	M. Persaud
	Japon	M. Yamazaki
	Malte	Mme Frazier
	Mozambique	M. Afonso
	Royaume-Uni de Grande-Bretagne et d'Irlande du Nord	Dame Barbara Woodward
	Sierra Leone	M. Kanu
	Slovénie	M. Žbogar
	Suisse	Mme Chanda

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)

24-17603 (F)

La séance est ouverte à 10 heures.

Adoption de l'ordre du jour

L'ordre du jour est adopté.

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)

Le Président (*parle en anglais*) : Je souhaite chaleureusement la bienvenue au Secrétaire général, ainsi qu'aux ministres et autres représentantes et représentants de haut niveau qui sont dans la salle du Conseil de sécurité. Leur présence aujourd'hui souligne l'importance de la question à l'examen.

Conformément à l'article 37 du règlement intérieur provisoire du Conseil, j'invite les représentantes et représentants des pays suivants à participer à la présente séance : Albanie, Allemagne, Arabie saoudite, Argentine, Australie, Autriche, Bahreïn, Bangladesh, Belgique, Brésil, Bulgarie, Cambodge, Chili, Costa Rica, Croatie, Cuba, Égypte, El Salvador, Émirats arabes unis, Espagne, Estonie, Gambie, Géorgie, Ghana, Grèce, Guatemala, Inde, Indonésie, Israël, Italie, Kazakhstan, Kiribati, Lettonie, Liechtenstein, Maroc, Népal, Norvège, Pakistan, Panama, Philippines, Pologne, Portugal, République islamique d'Iran, Roumanie, Singapour, Tchéquie, Türkiye, Ukraine, Uruguay et Viet Nam.

Conformément à l'article 39 du règlement intérieur provisoire du Conseil, j'invite les personnes ci-après, appelées à présenter un exposé, à participer à la présente séance : M. Stéphane Duguin, Directeur exécutif du CyberPeace Institute ; et M^me^ Nnenna Ifeanyi-Ajufo, professeur de droit et technologie à l'Université Beckett de Leeds.

Conformément à l'article 39 du règlement intérieur provisoire du Conseil, j'invite également les personnalités suivantes à participer à la présente séance : S. E. M^me^ Hedda Samson, Chargée d'affaires par intérim de la Délégation de l'Union européenne auprès de l'Organisation des Nations Unies ; M^me^ Roraima Ana Andriani, Représentante spéciale d'INTERPOL auprès de l'Organisation des Nations Unies ; et M^me^ Laetitia Courtois, Observatrice permanente et Cheffe de la Délégation du Comité international de la Croix-Rouge auprès de l'Organisation des Nations Unies.

Le Conseil de sécurité va maintenant aborder l'examen de la question inscrite à son ordre du jour.

J'appelle l'attention des membres du Conseil sur le document S/2024/446, qui contient le texte d'une 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, transmettant une note de cadrage sur la question à l'examen.

Je donne maintenant la parole au Secrétaire général, S. E. M. António Guterres.

Le Secrétaire général (*parle en anglais*) : Je remercie la République de Corée d'avoir organisé ce débat de haut niveau sur une question qui nous concerne toutes et tous, à savoir la paix et la sécurité dans le cyberespace.

Des technologies de l'information et des communications à l'informatique en nuage, en passant par la chaîne de blocs, les réseaux 5G, les technologies quantiques et bien d'autres innovations encore : les percées dans les technologies numériques se produisent à une vitesse fulgurante. Les avancées numériques révolutionnent les économies et les sociétés. Elles rassemblent les individus. Elles permettent de diffuser informations, nouvelles et connaissances et de s'instruire, sur simple commande tactile, ou d'un clic de souris. Elles offrent aux citoyennes et citoyens l'accès aux services et aux institutions de l'État, et elles dynamisent les économies, le commerce et l'inclusion financière.

Toutefois, de par sa qualité même, la connectivité fluide et instantanée qui fait du cyberespace une source d'avantages considérables peut aussi rendre les individus et les institutions, voire des pays entiers, profondément vulnérables. En outre, les dangers de voir les technologies numériques instrumentalisées à des fins hostiles s'accroissent d'année en année. Le cyberespace a ouvert de part en part des portes que tout un chacun peut franchir. Et c'est ce que beaucoup font. Les activités malveillantes dans le cyberespace, en augmentation, sont le fait d'acteurs aussi bien étatiques que non étatiques, tout comme de criminels proprement dits.

Les cyberincidents graves sont d'une fréquence inquiétante. Aux attaques portées aux services publics essentiels tels que les soins de santé, les services bancaires et les télécommunications, aux activités illicites

incessantes, menées notamment par des organisations criminelles et des « cybermercenaires », à la légion de marchands de haine qui polluent les autoroutes de l'information, y semant la peur et la discorde, et à l'utilisation croissante du cyberespace comme une nouvelle arme dans les conflits armés qui font rage, s'ajoute la présence d'« hacktivistes » civils qui, très souvent, brouillent la distinction entre combattants et civils. L'intégration croissante des outils numériques dans les systèmes d'armes, y compris les systèmes autonomes, est source de vulnérabilités inédites.

Dans le même temps, les détournements de la technologie numérique deviennent de plus en plus complexes et sournois. Les logiciels malveillants, les « wipers » et les chevaux de Troie prolifèrent. Les cyberopérations assistées par intelligence artificielle démultiplient la menace, et l'informatique quantique pourrait détruire des systèmes entiers par sa capacité de court-circuiter le chiffrement des données. Les vulnérabilités des logiciels sont exploitées, des moyens de cyberintrusion étant même vendus en ligne. Les chaînes d'approvisionnement des entreprises sont activement ciblées par des pirates informatiques, avec les graves perturbations en cascade que cela entraîne. Les rançongiciels sont un terrible exemple à cet égard en ce qu'ils représentent une menace considérable pour les institutions tant publiques que privées et pour les infrastructures essentielles dont elles dépendent. Selon certaines estimations, en 2023, le total des sommes versées à de tels logiciels en guise de rançon s'élevait à 1,1 milliard de dollars.

Cependant, le coût financier n'est rien par rapport au coup porté à notre paix, à notre sécurité et à notre stabilité communes, tant au sein des pays qu'entre eux. Les activités malveillantes qui sapent les institutions publiques, les opérations électorales et l'intégrité en ligne minent la confiance, alimentent les tensions et vont jusqu'à semer la violence et le conflit.

La technologie numérique offre une occasion extraordinaire d'édifier un avenir juste, plus équitable, durable et pacifique pour toutes et tous. Mais les avancées doivent être mises au service du bien. Le Nouvel Agenda pour la paix place la prévention au cœur de l'action pour la paix. Il y est prôné l'élaboration de cadres robustes conformes au droit international, aux droits humains et à la Charte des Nations Unies, et tous les États y sont exhortés à œuvrer activement pour empêcher l'expansion et l'escalade des conflits se déroulant dans le cyberespace ou par l'intermédiaire de celui-ci. Comme je l'ai indiqué dans ma nouvelle vision de l'état de droit, ce dernier est indispensable dans le domaine numérique comme dans le monde physique.

Je salue par ailleurs l'Assemblée générale, qui a montré qu'elle était déterminée à agir dans ce domaine. À cet égard, on peut notamment citer son groupe de travail à composition non limitée consacré à la sécurité du numérique et de son utilisation. Les États s'appuient sur le cadre normatif de comportement responsable qui leur est applicable dans l'utilisation de ces technologies, cadre qui a été entériné à l'unanimité. En outre, ils examinent activement la question de l'applicabilité du droit international aux activités qu'ils mènent dans ce domaine. Également sous les auspices de l'Assemblée générale, les États Membres œuvrent en vue de parvenir, dans les mois à venir, à un consensus sur un nouveau traité portant sur la cybercriminalité, ce qui devrait permettre de renforcer la coopération tout en protégeant les droits humains en ligne. Cependant, compte tenu des liens évidents qui existent entre le cyberespace et la paix et la sécurité mondiales, le Conseil peut également jouer un rôle majeur en intégrant les considérations relatives au cyberespace dans ses axes de travail et ses résolutions.

Ceci n'est que la deuxième séance officielle que le Conseil de sécurité tient sur la question. Pourtant, le cyberespace influence ou touche un nombre considérable de questions examinées autour de cette table, notamment la protection des civils en période de conflit armé, les opérations de paix, la lutte contre le terrorisme, ou encore les opérations humanitaires. En intégrant cette question à ses délibérations, le Conseil pourrait jeter les bases d'une action plus efficace dans cet important domaine.

(*l'orateur poursuit en français*)

Pour garantir la paix et la sécurité dans le monde physique, nous avons besoin de nouvelles approches sur la paix et la sécurité dans le monde numérique. Le Sommet de l'avenir qui se tiendra en septembre est une occasion vitale de renforcer la coopération sur les défis mondiaux essentiels et de revitaliser le système multilatéral. Le Pacte qui résultera du Sommet représente une chance unique de soutenir le maintien de la paix et la sécurité internationales dans le cyberespace. Entre autres priorités, le chapitre 2 du Pacte vise à réaffirmer un consensus mondial pour protéger les infrastructures critiques contre les pratiques numériques nuisibles, et renforcer la responsabilité de chacun concernant les technologies basées sur l'exploitation des données, y compris l'intelligence artificielle. Pendant ce temps, mon organe consultatif de haut niveau sur l'intelligence artificielle finalise son rapport sur la manière dont nous pouvons gouverner l'intelligence

artificielle pour l'humanité, en tenant pleinement compte des risques et des incertitudes. Je me réjouis de travailler avec le Conseil, l'Assemblée générale et l'ensemble des États Membres afin de faire en sorte que la technologie soit utilisée comme elle se doit : pour œuvrer au progrès et à la sécurité de toutes et tous et de la planète que nous partageons.

Le Président (*parle en anglais*) : Je remercie le Secrétaire général de son exposé.

Je donne maintenant la parole à M. Duguin.

M. Duguin (*parle en anglais*) : C'est un honneur pour moi que de m'adresser aujourd'hui au Conseil de sécurité sur une question d'une importance capitale : comment faire face à l'évolution des menaces dans le cyberespace. En tant que Directeur exécutif du CyberPeace Institute, organisation non gouvernementale, indépendante et neutre basée en Suisse, je parle en connaissance de cause puisque l'Institut propose des services gratuits de cybersécurité aux plus vulnérables, à savoir les organisations à but non lucratif, surveille les acteurs de la cybermenace, fournit des services de détection et d'analyse des menaces et mène des actions de plaidoyer pour le respect des lois et normes dans le cyberespace.

Tandis que nous analysons l'évolution des menaces, je voudrais aborder l'effet cumulatif résultant de perturbations graves du paysage de la menace qui, ensemble, ont une incidence directe sur le maintien de la paix et de la sécurité internationales. J'aborderai plusieurs sujets : la prolifération des acteurs de la cybermenace et la manière dont, en conséquence, les infrastructures critiques sont de plus en plus prises pour cible ; la mutation de la menace aujourd'hui, notamment avec la convergence des cyberattaques et de la désinformation et l'emploi de cyberattaques pour contourner les sanctions internationales ; et l'évolution de la menace de demain, qui s'accompagne du risque singulier que l'intelligence artificielle (IA) fait peser sur la cybersécurité. Ces évolutions génèrent des défis très particuliers pour la paix et la sécurité internationales, notamment en entravant l'attribution des responsabilités, c'est-à-dire le processus d'identification de l'auteur ou de la source d'une cyberattaque ou autre opération électronique.

Je commencerai par la prolifération des acteurs de la cybermenace. Depuis l'invasion de l'Ukraine par la Fédération de Russie en 2022, le CyberPeace Institute a recensé, documents à l'appui, une prolifération d'acteurs de la cybermenace dans les deux camps. La guerre n'est plus l'apanage des États. Un éventail d'acteurs non étatiques — groupes criminels, collectifs de « hacktivistes » aux motivations géopolitiques, et divers civils — prennent part à des cyberattaques et à des opérations dans le cadre de conflits armés. Ils poursuivent quatre objectifs : détruire les infrastructures, perturber le fonctionnement normal des services essentiels, synchroniser la désinformation et les cyberattaques, et voler des données et les instrumentaliser en recourant à l'infiltration et à l'espionnage. Dans ce contexte, le CyberPeace Institute a remonté la trace de plus de 3 000 campagnes de cyberattaques menées par 127 acteurs de la cybermenace, qui ont touché 56 pays et visé 24 secteurs d'infrastructures critiques. Les préjudices causés par ces cyberattaques ont été ressentis bien au-delà des frontières des pays belligérants, puisque près de 70 % de toutes ces cyberattaques ont eu une incidence sur des organisations situées dans des pays non belligérants. Ces données sont en libre accès sur notre portail « Cyber Attacks inTimes of Conflict » (Cyberattaques en temps de conflit). Cette prolifération d'attaques fait s'interroger sur la désescalade dans le contexte d'une éventuelle cessation des hostilités. Comment faire en sorte, dans de telles circonstances, que ces 127 acteurs de la cybermenace cessent leurs activités malveillantes ou soient maîtrisés ?

Cette prolifération a une incidence directe sur la sécurité des infrastructures critiques. Je donnerai deux exemples. En février 2022, une cyberattaque, utilisant un logiciel de type *wiper* appelé AcidRain, a pris pour cible l'accès par satellite de l'Ukraine à Internet à haut débit. Son impact a été ressenti au-delà des frontières de l'Ukraine. Elle a affecté le fonctionnement des éoliennes dans toute l'Europe : une grande entreprise allemande du secteur de l'énergie, par exemple, n'a plus pu surveiller à distance plus de 5 800 de ces éoliennes, et des milliers d'abonnés à des services Internet par satellite en Allemagne, en France, en Hongrie, en Grèce, en Italie et en Pologne ont été touchés. Ce type d'effet ne se fait pas sentir uniquement en période de conflit armé. Pendant la pandémie de maladie à coronavirus (COVID-19), le CyberPeace Institute a suivi 500 cyberattaques qui ont visé des établissements de santé pendant les deux années de la pandémie. Ces 500 cyberattaques ne représentent même pas la partie émergée de l'iceberg, elles sont à peine un glaçon au sommet de l'iceberg. À elles seules, ces 500 attaques ont perturbé les soins de santé dans 43 pays, ont entraîné le vol de données concernant 20 millions de patients, et se sont traduites par une interruption cumulée équivalente à cinq années d'accès aux soins de santé. Cela revient à un cumul de cinq années d'ambulances détournées, de

rendez-vous annulés et d'accès réduit aux soins de santé pour les patients.

Mais un autre aspect de cette évolution de la menace réside dans l'emploi de cyberattaques pour échapper aux sanctions internationales et financer des activités illégales. À titre d'exemple, divers acteurs de la société civile, organisations de cybersécurité et États ont analysé les activités de deux groupes criminels présumés, Kimsuky et le groupe Lazarus, dont les tactiques, outils, processus et intentions ont été attribués à la République populaire démocratique de Corée. Ces groupes criminels coordonnent des cyberattaques mondiales de tous types : attaques par logiciel rançonneur, ou attaques visant la chaîne d'approvisionnement, les plateformes d'échange de cryptomonnaies ou les institutions financières. Au-delà de l'important préjudice direct ou primaire de ces attaques, elles constituent un vecteur de contournement des sanctions internationales. Selon certaines estimations récentes, le groupe Lazarus et Kimsuky ont obtenu plus de 3 milliards de dollars grâce à ces attaques. Cette escalade cause des dommages considérables. L'attaque WannaCry, en mai 2017, qui a touché plus d'un quart de million d'ordinateurs en moins de 24 heures dans plus de 150 pays, a provoqué d'importantes perturbations et a été très lourde de conséquences pour les secteurs des soins de santé, des services financiers et des transports.

Pour terminer sur l'évolution des menaces, il est important d'anticiper sur les nouveaux risques, tels que la menace de l'informatique quantique pour la cryptographie ou, comme mentionné précédemment, l'influence de l'IA générative sur les modèles criminels. Depuis l'avènement de l'IA générative et des grands modèles de langage, l'IA est utilisée par des acteurs malveillants ne serait-ce que pour accroître leurs capacités. Aujourd'hui, l'IA sert à renforcer les processus existants dans ce qu'on appelle la « Kill Chain » de la cybersécurité, c'est-à-dire le processus standard que doit dérouler un attaquant pour mener une cyberattaque. Utiliser l'IA permet de gagner du temps pour identifier les cibles, automatiser la recherche des vulnérabilités ou augmenter les capacités de production des activités de hameçonnage, par exemple. Mais ce n'est qu'une première étape, et certains groupes expérimentent d'ores et déjà avec l'IA générative pour automatiser différents maillons d'une cyberattaque. Cela représente un risque inacceptable. Si les essais sont concluants, l'automatisation de la « Kill Chain » de la cybersécurité risque d'atteindre un niveau tel qu'un acteur malveillant pourrait, volontairement ou accidentellement, déclencher une cyberattaque autonome.

Compte tenu de la convergence de plusieurs perturbations cumulées — prolifération des menaces, nouveaux modes opératoires spécifiques pour attaquer les infrastructures critiques ou contourner les sanctions, et risques associés à la nouvelle technologie de l'IA —, il est difficile de riposter par une stratégie cohérente. Néanmoins, plusieurs mesures peuvent être prises, et je conclurai là-dessus.

Nous pouvons donner effet aux lois, aux normes et aux sanctions, notamment en recueillant de manière transparente des informations sur les violations et en adoptant une approche prospective pour prévenir l'utilisation malveillante du cyberespace, y compris l'utilisation abusive de l'IA ou de l'informatique quantique.

Il est important de dénoncer les auteurs d'infractions, de faire appliquer les sanctions et de prendre des mesures appropriées et adéquates. Il ne peut y avoir de désescalade sans déterminer les responsabilités, car cela est essentiel pour éclairer le processus décisionnel concernant les mesures à prendre et les moyens de défense à adopter. L'établissement des responsabilités peut avoir un effet dissuasif, dans la mesure où le fait d'amener les auteurs d'infractions à répondre de leurs actes peut faciliter l'adoption de mesures juridiques et diplomatiques et renforcer l'élaboration des politiques.

Enfin, il est indispensable de pouvoir mesurer de manière exhaustive et quantifiable les dommages causés par les cyberattaques. Le CyberPeace Institute est en train de mettre justement au point une méthodologie permettant de mesurer les dommages causés par les cyberattaques, car, jusqu'à présent, ils ont trop souvent été décrits en termes de perte d'argent ou de capacité, alors que les dommages causés aux populations humaines et aux structures sociales sont aussi importants.

Ces aspects sont essentiels au maintien de la paix et de la sécurité internationales.

Le Président (*parle en anglais*) : Je remercie M. Duguin de son exposé.

Je donne maintenant la parole à M^me^ Ifeanyi-Ajufo.

M^me^ Ifeanyi-Ajufo (*parle en anglais*) : C'est pour moi un privilège d'avoir été invitée à prendre la parole à la présente séance du Conseil sur le thème « Maintien de la paix et de la sécurité internationales : faire face à l'évolution des menaces dans le cyberespace », et plus particulièrement de pouvoir offrir une perspective régionale et examiner la situation en Afrique.

Dans toute discussion sur la paix et la sécurité dans le cyberespace, il est nécessaire de mesurer la sécurité du cyberespace à la lumière des réalités et des perspectives régionales. Nous devons prendre conscience du fait que les efforts visant à garantir la cybersécurité se heurtent souvent aux réalités des États en développement, en particulier ceux de la région africaine, qui sont toujours à l'extrémité de la fracture numérique et ne disposent pas des capacités, des compétences et des infrastructures adéquates pour garantir efficacement la paix et la sécurité selon les normes prévues. Par conséquent, tout en reconnaissant les éléments communs en matière de cybersécurité, nous devons aussi prendre conscience des différences et des défis qui existent entre les régions et envisager les cybermenaces en fonction des réalités propres à chaque pays et à chaque région.

Les dimensions de paix et de sécurité du cyberdomaine sont devenues un enjeu fondamental pour de nombreuses régions. Par exemple, en novembre 2022, le Conseil de paix et de sécurité de l'Union africaine a abordé pour la première fois la question de la paix et de la sécurité dans le cyberespace dans l'optique de la réglementer, dans le respect des règles du droit international. Par la suite, l'Union africaine a fait de la cybersécurité un programme phare de l'Agenda 2063 et un thème transversal de la Stratégie de transformation numérique pour l'Afrique (2020-2030). Fait important, la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, qui fournit un cadre réglementaire unifié pour atténuer les cybermenaces et protéger les infrastructures informatiques et de communication, est entrée en vigueur en juin 2023. En janvier de cette année, l'Union africaine a également adopté une position africaine commune sur l'application du droit international à l'utilisation des technologies de l'information et des communications dans le cyberespace. Je dois ajouter que la position africaine est le premier document de position sur l'application du droit international dans le cyberespace qui comprend une section sur le renforcement des capacités. L'Afrique est également la première région à avoir adopté une position commune régionale.

Nous devons aussi prendre conscience des nombreux défis qui se posent quant à la manière dont les régions peuvent maintenir la paix, la sécurité et la stabilité dans le cyberespace. Depuis l'année dernière, par exemple, nous avons été témoins de cyberattaques contre le siège de la Commission de l'Union africaine, qui ont compromis le fonctionnement des systèmes de courrier électronique. L'Autorité des communications du Kenya a annoncé que, pour la seule année 2023, le Kenya avait enregistré 860 millions de cyberattaques, dont des attaques sophistiquées visant les infrastructures d'information critiques du pays. Rien qu'en juillet 2023, le Kenya a été victime d'une cyberattaque très médiatisée visant la plateforme eCitizen, qui est très importante, attaque qui a rendu impossible l'accès à plus de 5 000 services gouvernementaux au niveau des ministères, des administrations des comtés et d'autres organismes. Un groupe qui se fait appeler Anonymous Sudan a revendiqué la responsabilité de ces cyberattaques au Kenya et ailleurs en Afrique. Il y a quelques mois, des cyberattaques organisées ont contraint le Gouvernement malawien à suspendre la délivrance des passeports, le réseau informatique du service de l'immigration ayant subi une cyberattaque qui a été qualifiée de grave atteinte à la sécurité nationale.

Cela soulève des questions importantes, notamment sur la frontière ténue entre la responsabilité des acteurs étatiques et celle des acteurs non étatiques, ainsi que sur la manière dont ces nouvelles cybermenaces viennent exacerber des conflits existants. Nous voyons que les conflits dans des régions comme l'Afrique favorisent les activités des groupes terroristes et extrémistes organisés. Nous constatons non seulement que les activités criminelles dans le cyberespace exacerbent les menaces et les défis qui pèsent sur la paix et la sécurité internationales dans la région, mais aussi que des États violent le droit international des droits de l'homme au nom de la cybersécurité en coupant l'accès à l'Internet, en particulier en période de conflit armé. Ces actes portent non seulement atteinte aux droits à la communication et à la liberté d'information des citoyens, mais font également obstacle à une action humanitaire efficace dans les situations de conflit dans des régions comme l'Afrique et, bien entendu, ailleurs. Nous constatons aussi que la désinformation et la mésinformation cybernétiques sont de plus en plus utilisées pour saper la paix et la sécurité en certains endroits de la région. Cette situation est encore aggravée par le recours à l'intelligence artificielle dans de telles circonstances.

Cependant, nous pensons que le Conseil de sécurité peut jouer un rôle déterminant dans le renforcement de la paix et de la sécurité dans le cyberespace, en particulier d'un point de vue régional. En effet, les sources d'inégalités existantes compliquent encore davantage la définition, par le Conseil de sécurité, d'un mandat sur la paix et la sécurité dans le cyberespace. Ces disparités en matière d'infrastructures de cybersécurité et de capacités numériques constituent un défi majeur, auquel s'ajoutent des conflits politiques persistants dans des régions comme l'Afrique. Par ailleurs, nous constatons une certaine

méconnaissance des obligations ayant trait à la non-intervention, à la diligence raisonnable et au règlement pacifique des différends dans le contexte du cyberespace.

Par conséquent, dans le cadre de la définition par le Conseil de sécurité de son mandat en matière de maintien de la paix et de la sécurité dans le cyberespace, il sera important d'envisager des mesures de collaboration efficaces permettant de contrer les menaces actuelles et de renforcer les capacités. Il est nécessaire d'établir et de renforcer les capacités au niveau régional. Cependant, nous devons souligner qu'il ne s'agit pas seulement d'une question de capacités juridiques, techniques et opérationnelles, mais aussi d'une question de réalités sociales, économiques et politiques. Au vu des différents niveaux de maturité en matière de cybersécurité et des différents contextes locaux, un renforcement stratégique des capacités régionales s'impose. Il faut tenir compte des réalités propres aux différentes régions, car les lacunes en matière de capacités ne sont pas nécessairement les mêmes d'une région à l'autre. Les initiatives visant à développer et à transférer les cybercapacités entre les régions doivent être menées dans le cadre d'une approche volontariste, mais également stratégique, en faisant fond sur des mécanismes d'établissement des responsabilités bien définis.

Dans des régions comme l'Afrique, la gouvernance, l'élaboration des politiques, les outils techniques et l'infrastructure, ainsi que la recherche, sont les domaines prioritaires où il convient de renforcer les capacités pour faire face aux cybermenaces. Il est indispensable de mettre en place les capacités nécessaires aux fins de la protection des infrastructures critiques. Il importe de veiller à ce que des équipes d'intervention en cas d'atteinte à la sécurité informatique soient mises en place au niveau régional là où elles n'existent pas encore, et de rendre obligatoire la création de points de contact régionaux accessibles 24 heures sur 24 et 7 jours sur 7. Il est aussi important d'élaborer et de mettre en œuvre des mécanismes permettant à ces équipes de collaborer au niveau régional et international.

Pour promouvoir la confiance et la sécurité dans le cyberdomaine, il faut se concentrer sur la mise en œuvre, dans toutes les régions, des normes de comportement responsable des États dans le cyberespace qui ont été définies par l'ONU. De nombreuses questions ont été soulevées quant au caractère volontaire de ces normes et à la nécessité d'adopter des approches plus responsables pour maintenir la paix et la sécurité dans le cyberespace, par exemple en définissant des lignes directrices claires sur l'usage de la force, les attaques armées et la légitime défense dans le cyberespace. Là encore, en créant et en appuyant des instances chargées d'élaborer des mesures de confiance, il sera possible de réduire la méfiance entre les États Membres et de faciliter le règlement pacifique des différends dans le cyberdomaine.

Il importe également que le Conseil de sécurité mette au point des mécanismes lui permettant d'appréhender les cybermenaces dans les différentes régions. Cette démarche permettra de prendre des décisions éclairées sur la réglementation relative à la sécurité et à la stabilité. À cette fin, un groupe de travail sur la paix et la sécurité dans le cyberespace pourrait être mis sur pied, lequel serait chargé, dans un premier temps, d'examiner les recommandations relatives aux conflits et à la promotion de la paix et de la stabilité dans le cyberespace. La mise en place de centres régionaux de cybersécurité qui fonctionnent comme il faut pour renforcer la coopération transfrontières et l'échange d'informations contribuera également à la réalisation de ces objectifs. Il convient également d'accorder une attention au renforcement des capacités pour l'élaboration et la mise en œuvre de stratégies régionales et nationales globales de cybersécurité, ainsi qu'à la promotion d'une culture de leadership en matière de cybersécurité.

Les organisations régionales ont un rôle clef à jouer dans la formulation des politiques et la collaboration avec les États de leur région afin d'obtenir des résultats en faveur de la paix et de la sécurité. Par conséquent, la coopération actuelle entre l'Organisation des Nations Unies et les organisations régionales et sous-régionales aux fins du maintien de la paix et de la sécurité internationales doit désormais inclure la cybersécurité. Enfin, le Conseil de sécurité doit promouvoir la création d'une instance qui permettra de mener un dialogue efficace pour encourager chaque région à élaborer un cadre pour la paix et la sécurité dans le cyberespace.

Je conclurai mon intervention en ajoutant qu'il sera essentiel pour le Conseil de sécurité de mettre en œuvre un programme multilatéral qui établit de manière décisive les dimensions de paix et de sécurité de l'état de droit dans le cyberespace. Cela nécessite également d'établir des principes et des normes de cybergouvernance bien définis qui obligeront toutes les régions et tous les gouvernements à rendre des comptes dans le domaine de la paix et de la stabilité. Au fur et à mesure que notre interdépendance et les conséquences des technologies de rupture, telles que l'intelligence artificielle, augmentent, notre vulnérabilité s'accroît également. Par conséquent, il est indispensable de renforcer nos capacités humaines et institutionnelles

pour sécuriser le cyberespace en renforçant la confiance dans l'utilisation des cybertechnologies.

Le Président (*parle en anglais*) : Je vais maintenant faire une déclaration en ma qualité de Ministre des affaires étrangères de la République de Corée.

Je tiens tout d'abord à remercier une nouvelle fois le Secrétaire général Guterres de sa présence et de son exposé d'aujourd'hui. Qu'il me soit également permis de remercier M. Stéphane Duguin, du CyberPeace Institute, et le professeur Nnenna Ifeanyi-Ajufo, de l'Université Beckett de Leeds, d'avoir partagé leurs vues et leur connaissances. Par ailleurs, je remercie vivement tous les représentants et toutes les représentantes des États Membres qui participent à ce débat public de haut niveau.

La séance d'aujourd'hui n'est que la deuxième fois dans l'histoire de l'ONU que le Conseil de sécurité se réunit officiellement pour discuter des menaces que le cyberespace fait peser sur la paix et la sécurité internationales. Le Conseil a organisé son tout premier débat public sur ce sujet il y a trois ans, en juin 2021 (voir S/2021/621). Certes, des étapes importantes ont été franchies en dehors du Conseil de sécurité. Les entités créées par l'Assemblée générale ont élaboré des normes de comportement responsable des États dans le cyberespace. Un certain nombre de réunions organisées selon la formule Arria ont également eu lieu sur la cybersécurité, la dernière en date étant la réunion d'avril, que la République de Corée a coorganisée avec les États-Unis et le Japon.

Le Secrétaire général a également fait preuve d'un leadership fort, en appelant à des mesures visant à atténuer les risques liés à la cybernétique et en créant l'Organe consultatif de haut niveau sur l'intelligence artificielle, dont la Corée fait partie. Mais les événements survenus depuis la première séance du Conseil de sécurité, il y a trois ans, soulignent clairement la raison pour laquelle le Conseil doit, aujourd'hui plus que jamais, renforcer activement sa mobilisation concernant les menaces provenant du cyberespace. Outre la myriade de cyberattaques transfrontières, le monde a été témoin du déclenchement de conflits armés majeurs au cours desquels des attaques ont été menées non seulement sur le champ de bataille traditionnel, mais aussi dans le cyberespace.

Le monde a également constaté la façon dont les progrès fulgurants de l'intelligence artificielle renforcent considérablement la capacité des acteurs malveillants de semer le chaos et de provoquer des perturbations dans le cyberespace. Le monde a vu comment les cyberactivités malveillantes peuvent avoir des répercussions concrètes en sapant la confiance dans l'intégrité des élections politiques, la sécurité des infrastructures critiques et le tissu de la paix et de la sécurité. D'ailleurs, un État Membre a même dû déclarer l'état d'urgence après avoir été victime d'attaques par logiciels rançonneurs provenant d'un autre pays.

Les cyberactivités sont fondamentalement à double usage : toute personne mal intentionnée peut introduire de nouvelles menaces ou déclencher, amplifier ou accélérer des menaces existantes. Comme l'a un jour fait remarquer Alvin Toffler, un célèbre futurologue, « nos pouvoirs technologiques augmentent, mais les effets secondaires et les dangers potentiels augmentent également ».

La République de Corée connaît bien les menaces que représentent les cyberactivités malveillantes et leurs conséquences sur la sécurité, étant donné que la mise au point des armes de destruction massive qui font peser des menaces sur la Corée est en grande partie financée par ces activités. Le dernier rapport en date du Groupe d'experts créé en application de la résolution 1874 (2009) (S/2024/215) indique que 40 % des programmes d'armes de destruction massive de la République populaire démocratique de Corée sont financés par des cyberactivités illicites. Le Groupe d'experts enquête sur une soixantaine de cyberattaques menées de 2017 à 2023, dont la République populaire démocratique de Corée est suspectée, visant des sociétés liées à des cryptomonnaies. Malheureusement, le Groupe n'existe plus, pour les raisons que nous connaissons tous.

Par des moyens numériques, la République populaire démocratique de Corée contourne systématiquement les sanctions adoptées par le Conseil et remet en cause le régime international de non-prolifération qui fait partie intégrante des travaux du Conseil. À une époque où la paix et la sécurité dans le monde physique et dans le cyberespace sont de plus en plus imbriquées, le Conseil de sécurité doit pas pratiquer la politique de l'autruche. Au minimum, il doit suivre le rythme des tendances extérieures et redoubler d'efforts pour faire face aux menaces réelles et actuelles provenant du cyberespace. Tout comme le Conseil de sécurité et l'Assemblée générale travaillent en synergie dans le cadre des discussions sur les armes de petit calibre, le terrorisme et la non-prolifération, le Conseil de sécurité et l'Assemblée générale peuvent également jouer des rôles complémentaires dans le domaine de la cybersécurité.

Même si aucune approche définitive concernant la voie à suivre n'a été encore adoptée, la République de

Corée voudrait soumettre les trois propositions suivantes au Conseil de sécurité pour examen.

Premièrement, le Conseil doit disposer d'une analyse claire de la situation actuelle. À cette fin, le Conseil de sécurité peut demander qu'on lui rende régulièrement compte de la situation, pour qu'il puisse examiner la façon dont les cybermenaces se recoupent avec son mandat et la façon dont l'évolution des cybermenaces influe sur la paix et la sécurité internationales.

Deuxièmement, les mesures qui seront prises devront porter sur l'ensemble des dossiers du Conseil. La cybersécurité pourrait être intégrée aux travaux du Conseil de la même manière que d'autres questions transversales, telles que les femmes et la paix et la sécurité, les jeunes et les changements climatiques. Comme l'ont souligné de nombreux États Membres à la réunion organisée selon la formule Arria en avril, il existe un lien direct entre les utilisations malveillantes des technologies de l'information et des communications et les différentes questions relevant de la compétence du Conseil de sécurité, notamment les sanctions, la non-prolifération et le terrorisme. Dans cette optique, le Conseil peut considérer la cybersécurité comme un aspect majeur qui concerne l'ensemble des questions ou dossiers régionaux et thématiques dont il est saisi.

Troisièmement, et à moyen et à long terme, le Conseil de sécurité doit pouvoir trouver un moyen approprié de faire face à ce problème. Le Conseil peut organiser des séances sur les cyberactivités malveillantes qui violent le droit international et nuisent à la paix et à la sécurité. En outre, il pourrait exhorter tous les acteurs concernés à utiliser les cybertechnologies de manière responsable et à demander des comptes en utilisant les outils à la disposition du Conseil. Il va sans dire que le Conseil de sécurité doit élaborer un programme de travail sur la cybersécurité, qui complète les discussions en cours à l'Assemblée générale.

Le Conseil de sécurité a toujours défini ses priorités, en fonction de l'émergence de nouveaux problèmes de sécurité. Les architectes de la Charte des Nations Unies étaient loin d'imaginer que les changements climatiques, les atteintes aux droits humains et les pandémies allaient relever de la compétence du Conseil de sécurité. Le Conseil de sécurité doit prendre la question de la cybersécurité à bras le corps s'il veut rester pertinent et agile face à l'un des problèmes de sécurité les plus pressants de notre époque. J'espère sincèrement que le débat public d'aujourd'hui suscitera un élan en ce sens.

Avant de conclure mon intervention, je voudrais simplement ajouter un dernier point. Étant donné que le cyberespace n'a pas de frontières, aucun pays, qu'il soit avancé ou vulnérable sur le plan numérique, n'est à l'abri des dégâts de la cybermalveillance. La solidité de la sécurité internationale dans le cyberespace se mesure à celle de son maillon le plus faible. Par conséquent, le lien entre l'action humanitaire, le développement et la paix n'est pas moins réel dans le cyberespace. Un cyberespace exempt de cyberactivités malveillantes facilitera le développement numérique et ouvrira des perspectives numériques qui contribueront, à terme, à la réalisation des objectifs de développement durable. Un cyberespace ouvert, sûr, accessible et pacifique, dans lequel les cybermenaces peuvent être efficacement dissuadées, protégera également la liberté et les droits humains en ligne.

Je reprends à présent mes fonctions de Président du Conseil de sécurité.

Je donne maintenant la parole à S. E. M^me^ Linda Thomas-Greenfield, Représentante permanente des États-Unis et membre du Cabinet du Président Biden.

M^me^ Thomas-Greenfield (États-Unis d'Amérique) (*parle en anglais*) : Je tiens tout d'abord à remercier la République de Corée de nous avoir réunis une nouvelle fois pour discuter de cette question cruciale qui relève de la paix et de la sécurité. Je vous souhaite la bienvenue au Conseil de sécurité, Monsieur le Président, et vous exprime toute ma reconnaissance. J'ai eu l'honneur de vous rencontrer à Séoul lors de ma visite il y a quelques mois, et je suis ravie de vous retrouver ici. Je remercie le Secrétaire général et les intervenants de leurs exposés et je souhaite la bienvenue aux autres ministres, qui nous font l'honneur de leur présence aujourd'hui.

Depuis notre séance précédente en avril, nous sommes convaincus qu'il est impératif d'assurer une sécurité solide dans le cyberespace et qu'il faut donc examiner cette question au Conseil. La cybersécurité permet à nos systèmes fondamentaux de fonctionner, qu'il s'agisse de nos économies, de nos institutions démocratiques ou de l'ONU elle-même. Les États-Unis sont déterminés à travailler avec tous les acteurs responsables pour préserver les avantages du cyberespace, renforcer la solidarité numérique et tirer parti de la technologie afin de réaliser les objectifs de développement durable. Et pourtant, beaucoup trop d'acteurs étatiques et non étatiques agissent dans le sens inverse. Dans le monde entier, ils exploitent la connectivité numérique pour extorquer des victimes à des fins lucratives, voler de l'argent et des idées aux gouvernements et aux entités privées, attaquer des journalistes

et des défenseurs des droits humains, se préparer à de futurs conflits et menacer nos infrastructures critiques, y compris ici, à l'ONU.

En tant que Conseil, nous devons œuvrer de concert pour faire face aux cybermenaces posées par les acteurs étatiques et non étatiques et renforcer les normes de comportement responsable des États, demander des comptes aux pays qui ont des comportements irresponsables dans le cyberespace et soutenir les victimes touchées par ces comportements, et pour perturber les réseaux criminels qui sont à l'origine de cyberattaques dangereuses dans le monde entier. Il existe déjà un cadre pour ce faire. Le cadre de comportement responsable des États dans le cyberespace, adopté à plusieurs reprises et par consensus, indique clairement que le droit international s'applique au cyberespace et que les États sont censés respecter les normes facultatives de comportement des États en temps de paix. Parmi ces normes, on attend des États qu'ils enquêtent sur les cyberactivités malveillantes émanant de leur territoire et visant les infrastructures critiques d'autres États, et qu'ils en atténuent les effets. Pourtant, certains de ceux qui ont approuvé ce cadre choisissent de fermer les yeux sur les agissement des acteurs malveillants ou, pire, de leur donner les moyens d'agir.

C'est ce qui a été souligné lors de la réunion organisée selon la formule Arria en avril, notamment les cyberopérations malveillantes menées par la République populaire démocratique de Corée et utilisées pour financer ses programmes d'armes de destruction massive et de missiles balistiques. Il convient également de mentionner les cyberactivités de la Russie en Ukraine, en Allemagne, en Tchéquie, en Lituanie, en Pologne, en Slovaquie et en Suède, où, entre autres activités, la direction principale du renseignement de l'état-major de la Russie cible les partis politiques et les institutions démocratiques. En outre, le Gouvernement russe offre également un refuge aux concepteurs de rançongiciels qui, ces dernières années, ont causé des milliards de dollars de pertes et des dommages considérables aux hôpitaux et à d'autres infrastructures critiques.

De leur côté, les États-Unis et le Royaume-Uni ont annoncé en février des opérations visant à perturber le groupe de rançongiciels LockBit, qui a 2 000 victimes à son actif et a demandé des centaines de millions de dollars de rançon, dont plus de 120 millions ont été versés. Ces derniers mois, nous avons levé les scellés d'un acte d'accusation visant les ressortissants russes Artur Sungatov et Ivan Kondratyev, également connus sous le nom de Bassterlord, pour avoir déployé LockBit contre de nombreuses victimes aux États-Unis et dans le monde entier. Cela vient s'ajouter aux efforts déployés dans le cadre de l'Initiative internationale de lutte contre les rançongiciels que nous avons mise en place en 2021 et qui est aujourd'hui le plus grand cyberpartenariat au monde. En tant qu'États à titre individuel, dans le cadre de ce partenariat et dans les enceintes multilatérales, y compris à l'ONU, nous appelons tous les États à jouer leur rôle pour appliquer ce cadre et promouvoir la paix et la stabilité dans le cyberespace. Nous demandons au Conseil de veiller à ce que la cybersécurité soit une priorité transversale prise en compte dans tous les aspects de notre mandat. Qu'il s'agisse d'examiner la manière dont les opérations de maintien de la paix peuvent promouvoir une bonne cyberhygiène pour limiter les risques ou de mieux comprendre comment la cybersécurité pourrait renforcer les efforts de non-prolifération, le Conseil doit continuer à envisager les problèmes sous l'angle de la cybersécurité.

Nous avons la capacité de protéger nos infrastructures les plus critiques et tous ceux qui en dépendent. Et nous avons la possibilité de préserver les avantages du cyberespace pour tous. Ainsi, en nous inspirant du cadre de comportement responsable des États dans le cyberespace, nous devons réaffirmer l'applicabilité du droit international au comportement des États entre eux. Nous devons encourager l'adhésion à des normes facultatives de comportement responsable des États en temps de paix et contribuer à réduire le risque que des conflits n'éclatent à la suite de cyberincidents. Nous devons également faire respecter l'ordre international fondé sur des règles et veiller à ce que le monde numérique permette d'améliorer le monde physique.

Je vous remercie une fois de plus, Monsieur le Président, de nous avoir réunis pour aborder ce sujet important.

M. Persaud (Guyana) (*parle en anglais*) : Je remercie S. E. M. Cho Tae-yul, Ministre des affaires étrangères, et la présidence coréenne du Conseil de sécurité d'avoir organisé le débat public d'aujourd'hui sur l'évolution des menaces dans le cyberespace. Je remercie également le Secrétaire général et les intervenants de leurs contributions éclairantes à ce débat.

L'évolution rapide des technologies a créé un monde aux possibilités illimitées, avec d'énormes avantages économiques, sociaux et géopolitiques. Cependant, à mesure que les technologies numériques deviennent plus sophistiquées et sont déployées par des acteurs malveillants, elles posent des risques sans précédent pour la sécurité humaine et nationale. L'utilisation

malveillante des technologies numériques a également montré que celles-ci pouvaient perturber les institutions et poser des problèmes réglementaires et politiques liés à la gouvernance. En outre, la nature transnationale des cybermenaces a rendu obsolètes les notions traditionnelles de sécurité et de défense nationales.

Les menaces de cybersécurité auxquelles nous sommes exposés aujourd'hui peuvent avoir des conséquences désastreuses sur la santé, la sûreté et la sécurité de nos concitoyens, ainsi que sur le fonctionnement des services essentiels. Les menaces contemporaines qui pèsent sur la cybersécurité deviennent de plus en plus sophistiquées et multiformes, qu'il s'agisse du cyberespionnage parrainé par les États, de l'ingérence dans les processus démocratiques, des violations des droits humains, d'attaques contre les infrastructures critiques ou de la diffusion de fausses informations, de désinformation et de discours de haine, et notre riposte doit l'être également.

À cet égard, je suggère d'examiner trois questions.

Premièrement, il faut mettre en place des mécanismes d'application du principe de responsabilité et de surveillance pour nous prémunir contre les cyberattaques. À cet égard, nous prenons note des discussions récentes sur la question de savoir si les cyberattaques dirigées contre des infrastructures critiques, telles que des installations médicales ou des centrales électriques, avec de graves conséquences pour la vie, peuvent constituer des crimes de guerre, des crimes contre l'humanité, un génocide et/ou des crimes d'agression. Cette question doit faire l'objet d'un examen approfondi et être incorporée à un cadre juridique mondial qui doit également garantir que les outils et les technologies numériques sont mis au point et utilisés dans le respect des considérations éthiques et des droits humains. À cet égard, le Guyana reconnaît l'importance de mener à bien les travaux 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 et la nécessité d'une convention ratifiée par de nombreuses parties.

Deuxièmement, nous devons donner la priorité à la coopération, à la collaboration et aux partenariats afin de renforcer les capacités et la résilience en matière de cybersécurité, d'enquêter sur les cybercrimes dans tous les pays et toutes les régions et d'en poursuivre les auteurs. En termes de partenariats, nous devons investir dans l'instauration de la confiance et le renforcement de la collaboration régionale et internationale afin de favoriser le partage des connaissances, l'échange d'informations et le transfert de technologies. Nous devons également chercher à développer l'interopérabilité entre nos systèmes nationaux, régionaux et internationaux qui s'occupent du suivi et de la surveillance des menaces de cybersécurité. Pour être efficace, il faut élaborer un cadre mondial qui permette aux États et aux parties prenantes concernées d'échanger des informations sur les nouvelles menaces qui pèsent sur la cybersécurité. Si les discussions en cours à l'ONU et au sein des mécanismes régionaux ont contribué positivement à cet effort, notamment dans le cadre du Plan d'action de coopération numérique du Secrétaire général et du Programme d'accélération numérique au service des objectifs de développement durable, il reste beaucoup de travail à accomplir. Nous devons également tirer parti des possibilités offertes par le cyberdomaine pour adopter une approche globale de la société afin de contrer les cybermenaces et de renforcer la cybersécurité.

Les nouvelles technologies, telles que les systèmes d'intelligence artificielle, peuvent contribuer à identifier et à atténuer ces menaces. À cet égard, les gouvernements doivent redoubler d'efforts pour collaborer avec les entreprises technologiques et le secteur privé afin de mettre au point des outils et des politiques de sécurité plus solides et d'améliorer le partage de l'information dans l'analyse des renseignements sur les cybermenaces. Par ailleurs, de nombreux pays en développement tels que le Guyana ne disposent pas des ressources et des compétences nécessaires pour lutter contre les cybermenaces et devenir plus résilients. Le renforcement des capacités techniques de ces pays doit être considéré comme un investissement dans notre sécurité collective qui permettrait d'éliminer les inégalités et les déséquilibres existants en termes de capacités en matière de cybersécurité. À cet égard, en tant que communauté mondiale, nous pourrions réfléchir à la possibilité de créer un fonds mondial destiné à la formation et au renforcement des capacités, ainsi qu'à la mise au point de logiciels et de matériel informatique. En outre, le Guyana exhorte les pays développés dotés de capacités technologiques avancées à fournir une assistance technique et un financement pour améliorer l'infrastructure de cybersécurité et les capacités de réponse des pays en développement. En outre, il ne faut ménager aucun effort pour veiller à ce qu'aucun pays ou entité ne monopolise les outils et les capacités technologiques qui pourraient exacerber les vulnérabilités des pays en développement, par exemple par l'imposition de lois et de réglementations ayant des effets extraterritoriaux.

Troisièmement, nonobstant les processus en cours dans d'autres instances onusiennes, le Conseil de

sécurité doit participer au dialogue sur la cybersécurité, compte tenu de la menace que représente la cyberactivité malveillante pour le maintien de la paix et de la sécurité internationales. Le Conseil doit donc intensifier ses discussions sur cette question en s'appuyant sur les réunions organisées selon la formule Arria et les débats publics, y compris le présent débat, afin de sensibiliser aux menaces émergentes posées par les nouvelles technologies et d'examiner, collectivement, les mesures efficaces qui peuvent être déployées contre l'emploi malveillant de ces technologies.

Pour terminer, les défis posés par les menaces de cybersécurité sont redoutables mais pas insurmontables. Grâce à nos efforts et à notre volonté collectifs, ainsi qu'à une action concertée, nous pouvons construire un monde numérique résilient et sûr qui favorise la confiance, l'innovation et la prospérité pour tous et toutes. Saisissons cette occasion, non seulement pour répondre aux menaces qui pèsent sur nous, mais aussi pour activement façonner un avenir qui ne laissera personne de côté. Le Guyana est prêt à collaborer avec tous les États Membres pour atteindre cet objectif.

M. Nebenzia (Fédération de Russie) (*parle en russe*) : C'est un plaisir de vous accueillir ici, Monsieur le Président, à la présidence du Conseil de sécurité. Nous remercions le Secrétaire général de son exposé. Nous avons écouté attentivement les exposés des intervenants.

La Fédération de la Russie a été à l'origine du débat sur les questions de sécurité internationale de l'information à l'ONU. En 1998, il y a 26 ans, nous avons soulevé pour la première fois le sujet à l'Assemblée générale, en présentant la première résolution dédiée à cette question (résolution 53/70 de l'Assemblée générale). L'adoption de ces résolutions est depuis lors devenue un événement annuel et bénéficie de l'appui de l'écrasante majorité des États Membres.

À notre initiative, un groupe d'experts gouvernementaux des Nations Unies a été créé pour examiner les questions de sécurité liées à l'utilisation des technologies de l'information et des communications (TIC). Il a par la suite évolué vers un format inclusif pour devenir le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), qui est l'unique instance de négociation sous les auspices des Nations Unies chargée d'aborder toutes les questions liées à la sécurité de l'information au niveau international.

Depuis qu'il a été créé, le groupe de travail à composition non limitée a prouvé son efficacité et sa pertinence. Parmi ses résultats concrets, on peut citer le lancement en mai, à l'initiative de la Russie, d'un répertoire de points de contact pour l'échange d'informations sur les attaques ou incidents informatiques. Un examen détaillé des menaces existantes et potentielles dans le domaine de la sécurité internationale de l'information est en cours. Des mesures concrètes sont prises pour renforcer les capacités numériques des États. L'année dernière, des principes universels d'assistance dans ce domaine ont été adoptés.

Nous sommes convaincus que les efforts de la communauté internationale doivent se concentrer sur la poursuite du renforcement de la coopération entre les États dans le cadre du groupe de travail à composition non limitée, afin d'obtenir des résultats concrets et pratiques pour garantir la sécurité de l'information au niveau international. Nous pensons qu'il est essentiel de consolider et d'exploiter les résultats obtenus par le groupe de travail à composition non limitée, tant dans le cadre de son mandat actuel que dans celui d'un futur format de négociation. La Russie a déjà présenté sa vision d'un mécanisme inclusif permanent dans ce domaine. Nous considérons qu'il serait judicieux de préserver nos acquis communs en établissant un groupe de travail permanent à composition non limitée doté d'une fonction décisionnelle après 2025.

Ces faits démontrent clairement que l'ONU mène depuis longtemps un travail cohérent et progressif en matière de sécurité internationale de l'information. C'est pourquoi la nécessité d'impliquer le Conseil de sécurité soulève de sérieuses questions. Le sujet a ses propres spécificités et doit être abordé dans des instances spécialisées qui disposent de compétences spécialisées nécessaires. Il est essentiel que les discussions restent professionnelles et constructives, en évitant toute politisation. La duplication des efforts de la communauté internationale et l'éparpillement du sujet dans les différentes plateformes des Nations Unies sont contre-productives et pourraient compromettre les résultats obtenus au fil des décennies sous les auspices de l'Assemblée générale.

Il est tout aussi important que les discussions du groupe de travail à composition non limitée soient inclusives. Tous les Membres de l'ONU sans exception y sont associés, sur un pied d'égalité, puisque les décisions sont prises par consensus. Le transfert de la question au Conseil de sécurité exclurait automatiquement de la prise de décision tous les États qui ne sont pas membres du Conseil. Ceux qui ont soutenu aujourd'hui l'appel de la présidence à inscrire la sécurité internationale de

l'information à l'ordre du jour du Conseil de sécurité doivent en avoir conscience.

Enfin, toute discussion sur les risques potentiels doit tenir compte des particularités technologiques du cyberespace. Contrairement au monde physique, les menaces dans le cyberespace sont extrêmement difficiles à cerner, sans parler de l'identification de la source d'une attaque, que l'on appelle l'attribution. Il faut souvent beaucoup de temps pour se rendre compte qu'une attaque a eu lieu, et encore par des preuves indirectes, . Par conséquent, à l'heure actuelle, nous ne savons même pas avec certitude quels sont les cas d'utilisation malveillante des TIC qui peuvent être considérés comme des menaces directes pour la paix et la sécurité internationales. Tant que le problème de l'attribution n'aura pas été résolu et qu'une approche unifiée n'aura pas été adoptée pour les autres aspects complexes de ce problème spécifique aux multiples facettes, y compris les aspects juridiques, toute discussion au sein du Conseil de sécurité pourrait se transformer en un nouvel échange d'accusations non fondées et entraîner des divisions encore plus profondes au sein de la communauté internationale. Cela saperait l'autorité du Conseil et ne contribuerait en rien à l'élaboration de solutions constructives.

Tous les États qui se sont exprimés ou qui s'exprimeront aujourd'hui participent au groupe de travail à composition non limitée, et les questions proposées pour ce débat sont similaires à celles qui sont examinées au sein du groupe. Une table ronde sur le renforcement des capacités dans le domaine de la sécurité internationale de l'information a été organisée au niveau ministériel en mai, et la huitième session du groupe de travail à composition non limitée aura lieu en juillet. En fait, la discussion sur le sujet est déjà en cours et ses progrès et résultats sont accessibles à tous.

C'est pourquoi nous ne soutenons pas l'appel visant à sensibiliser la communauté internationale aux questions de sécurité internationale de l'information en organisant des séances régulières du Conseil de sécurité. Le mandat du Conseil de sécurité implique une réponse rapide aux menaces réelles qui pèsent sur la paix et la sécurité internationales, et non un échange de vues philosophique sur des sujets populaires dans le domaine public. Il existe d'autres forums et formats pour cela.

Les tentatives de nos collègues occidentaux de faire des allégations d'activités malveillantes dans l'espace numérique, et de s'en servir comme moyen de pression contre les États qu'ils jugent indésirables sont extrêmement préoccupantes, d'autant qu'ils ne présentent jamais aucune preuve convaincante pour étayer leurs propos.

Le Groupe d'experts du Comité du Conseil de sécurité créé par la résolution 1718 (2006) concernant la République populaire démocratique de Corée, a été maintes fois instrumentalisé dans ce jeu sans scrupules. Se fondant sur un tuyau émanant d'un État Membre, le Groupe a contacté la Russie au sujet d'attaques informatiques attribuées à Pyongyang. Lorsque nous avons demandé les données précises requises pour enquêter sur les incidents allégués, les experts ont répondu qu'ils n'avaient reçu aucune information supplémentaire de leur « source ». Cette absence de précisions n'empêche cependant pas nos collègues occidentaux d'accuser, sans fondement, les pays qui désapprouvent leurs actions de tous les « cyberpéchés », en recourant à leur qualificatif favori : « hautement probable ». Ces insinuations infondées sont inacceptables. L'attribution des responsabilités exige une démarche professionnelle et la fourniture de preuves techniques exhaustives.

Nous rejetons catégoriquement les spéculations selon lesquelles la Russie encouragerait des actions malveillantes dans le cyberespace. Cela fait un quart de siècle que nous plaidons pour prévenir la militarisation du cyberespace, et nos premières propositions concrètes dans ce sens sont intervenues longtemps avant que les pays occidentaux aient même pris conscience de ce risque.

Pour notre pays, la priorité est d'élaborer des instruments universels juridiquement contraignants sur la sécurité du numérique, car ils contribueront à prévenir les conflits interétatiques dans cet espace. Dans ce sens, la Russie a déposé à l'Assemblée générale, en 2023, un prototype de traité international spécialisé. Il s'agissait d'un concept de convention sur les moyens de garantir la sécurité internationale de l'information. L'adoption d'un tel accord universel permettrait non seulement de formaliser juridiquement les droits et obligations des pays s'agissant de leurs activités dans le domaine du numérique, mais aussi de régler le problème de l'attribution des responsabilités politiques en cas d'attaque informatique dans les relations internationales. Cela contribuerait également à assurer le strict respect, dans l'espace numérique, du principe de l'égalité souveraine des États qui, à l'heure actuelle, est ouvertement méprisé par de nombreux pays technologiquement avancés. Nous invitons tous les États Membres à engager, à l'Assemblée générale, un dialogue de fond sur la base de notre proposition.

Malheureusement, les pays occidentaux, États-Unis en tête, rejettent cette idée, car ils cherchent à préserver au

maximum leur liberté d'action. Ceci est particulièrement évident, vu que des hauts fonctionnaires des États-Unis ont reconnu des opérations numériques offensives menées contre la Russie, et que les doctrines de Washington et de l'OTAN prévoient des approches dites offensives et, en réalité, agressives.

Nos intervenants d'aujourd'hui et les délégations qui ont pris la parole jusqu'ici ont évoqué des cyberattaques. Ils ont toutefois oublié de dire qu'une guerre de la désinformation sans précédent est actuellement livrée contre la Russie. Toute cette activité malveillante est coordonnée depuis la Grande-Bretagne par des organisations basées à Londres, comme la « Public Relations and Communications Association », le « PR Network », ou encore la « IT Army of Ukraine », qui mène sans relâche des activités de désinformation. Avec l'aide de ces ressources informatiques, des tonnes de désinformation et de mensonges sur la Russie et son opération militaire spéciale sont déversées dans l'espace numérique.

Les tentatives d'édulcorer le débat mondial sur la lutte contre l'exploitation du numérique à des fins criminelles sont également alarmantes. À titre d'exemple éloquent, citons l'Initiative de lutte contre les rançongiciels. Ces « clubs exclusifs », qui ne cherchent pas particulièrement à dissimuler leurs objectifs politisés, sapent les efforts déployés par les États Membres pour mettre au point des mécanismes universels de lutte contre l'utilisation du numérique à des fins criminelles, notamment via 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.

Depuis plus de 26 ans maintenant, la Fédération de Russie promeut un programme constructif dans le domaine de la sécurité internationale de l'information, contribuant ainsi au maintien de la paix et de la stabilité dans les mondes aussi bien réel que virtuel. Nous continuerons de défendre les principes visant à créer un environnement numérique pacifique et sûr à l'échelle mondiale.

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.

M. Afonso (Mozambique) (*parle en anglais*) : Le Mozambique tient à vous remercier, Monsieur le Président, ainsi que la République de Corée, d'avoir choisi ce thème important pour la manifestation phare de votre présidence du Conseil de sécurité en ce mois de juin. Nous sommes profondément reconnaissants au Secrétaire général de son approche extrêmement édifiante sur ce sujet, d'autant qu'elle s'aligne très judicieusement sur la Charte des Nations Unies. Nous avons suivi avec une grande attention les éclairages importants fournis par M. Stéphane Duguin, Directeur exécutif du CyberPeace Institute, et par M^me^ Nnenna Ifeanyi-Ajufo, professeure de droit et technologie.

Nous saluons les ministres et hauts dignitaires présents dans la salle aujourd'hui.

Toutes les déclarations faites jusqu'ici témoignent du fait que les frontières entre le cyberespace et le monde physique continuent de s'estomper rapidement. En conséquence, pratiquement toutes les facettes de notre vie moderne ont migré vers la technologie numérique, dont elles dépendent. La nécessaire implication du Conseil est donc étayée par le fait que de nombreux pays, grands et petits, envisagement sérieusement le cyberespace, qui n'a pas de frontières, comme un domaine de conflit possible, au même titre que la terre, les mers, l'air et l'espace.

En l'occurrence, nous pouvons prendre pour point de départ le fait que, en 2013, l'Assemblée générale a convenu que le droit international, y compris la Charte des Nations Unies, s'applique bien au cyberespace. Néanmoins, les échanges diplomatiques mondiaux autour des règles d'engagement dans le cyberespace n'ont, jusqu'ici, progressé que lentement. À cet égard, les discussions menées sous les auspices du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) n'ont pas encore donné de résultats.

Le panorama et l'ampleur des cybermenaces évoluent rapidement, marqués par les progrès rapides de l'intelligence artificielle, et par d'importantes nouvelles menaces pour la paix, la sécurité et la stabilité nationales et internationales. Avec la montée en puissance des cybermenaces, il ne se passe pas un jour ou presque sans attaque par rançongiciel contre des entités publiques ou privées, sans prolifération d'hypertrucages générés par intelligence artificielle et qui semblent tout à fait réels, ou sans tentative d'attaque par déni de service contre certains éléments ou services essentiels d'un pays, tels que le secteur financier, les soins de santé, les réseaux électriques, l'administration en ligne et autres infrastructures critiques. Tandis que les outils mis au point pour faciliter la vie moderne sont utilisés à mauvais escient et instrumentalisés, la cybercriminalité est devenue un multiplicateur de menace parmi les plus importants en

sapant la confiance du public dans les institutions et en amplifiant les tensions politiques et sociales.

Ces défis sont aggravés par l'intensification de la concurrence géopolitique, qui est devenue un facteur important dans le domaine de la cybersécurité. Des adversaires s'efforcent d'acquérir des cybercapacités militaires et de renseignement, ce qui déclenche une course aux cyberarmements dans un contexte marqué par l'intensification des accusations, des mises en cause, des représailles et de l'escalade. Alors que la cybersécurité se mêle de plus en plus à la géopolitique, les perspectives de faire des progrès en vue de parvenir à un accord international sur de meilleures normes de cybersécurité restent dans l'impasse, et deviennent de plus en plus lointaines. Cet immobilisme ou ce manque de progrès sur une question aussi importante pour l'humanité risque de compromettre notre sécurité collective.

Compte tenu de l'évolution rapide des menaces et de l'absence de règles d'engagement adoptées d'un commun accord, le Conseil de sécurité doit assumer certains rôles et mener des activités spécifiques de toute urgence.

Premièrement, il doit établir des normes et des cadres internationaux relatifs au comportement responsable des États et des entités privées dans le cyberespace, sur la base d'une coopération mondiale.

Deuxièmement, dans le but de favoriser notre sécurité collective, le Conseil pourrait appuyer des initiatives de renforcement des capacités afin d'améliorer les capacités de cyberdéfense des États Membres, en particulier ceux dont les ressources sont limitées.

Troisièmement, le Conseil pourrait promouvoir la tenue de séances d'information sur l'appréciation de certaines situations, et faciliter l'échange de renseignements sur les menaces et de bonnes pratiques entre les nations afin de renforcer notre résilience commune en matière de cybersécurité.

Quatrièmement, il convient d'établir systématiquement un lien entre les cybermenaces et d'autres questions dont le Conseil de sécurité est saisi, telles que la lutte contre le terrorisme, l'ingérence dans les élections, la protection des infrastructures critiques et la sauvegarde des opérations de paix et de l'action humanitaire.

Nous pensons qu'il est primordial d'actualiser et d'élargir le débat sur la cybersécurité. Les questions liées au vol d'idées, de données et de propriété intellectuelle, aux droits humains et à la vie privée, ainsi qu'aux paramètres de conception des produits de consommation essentiels et des services d'utilité publique, méritent le même niveau d'attention. Pour des pays comme le Mozambique, il est impératif que les voix et les points de vue du monde du Sud soient entendus dans le débat mondial sur la cybersécurité. La diversité des points de vue et le rejet des solutions toutes faites sont indispensables pour progresser, au niveau mondial, vers un cadre de gouvernance plus équitable et plus résilient. En encourageant des discussions telles que celle que nous sommes en train de mener sous la présidence de la République de Corée, le Conseil peut jouer un rôle central dans la préservation de la paix et de la sécurité internationales à l'ère numérique. Le Mozambique s'engage à rester mobilisé sur cette question.

M. Kanu (Sierra Leone) (*parle en anglais*) : Je vous remercie, Monsieur le Président, d'avoir organisé cet important débat public. Je tiens également à remercier le Secrétaire général, S. E. M. António Guterres, de son exposé éclairant. Nous remercions aussi M. Stéphane Duguin et M^me^ Nnenna Ifeanyi-Ajufo de leurs observations. Nous nous félicitons de la participation des ministres de haut rang à la présente séance.

La Sierra Leone se réjouit de l'occasion qui lui est donnée de s'exprimer sur la question cruciale de l'évolution des menaces dans le cyberespace, tout en reconnaissant les immenses avantages et les défis interdépendants que les technologies de l'information et des communications (TIC) représentent pour la paix et la sécurité internationales. Nous sommes également conscients de l'enjeu fondamental que représente, pour le développement, la réduction de la fracture numérique mondiale, ainsi que du risque d'aggravation de cette fracture du fait de la prolifération de l'intelligence artificielle (IA), en particulier de l'IA générative.

Dans cette déclaration, la Sierra Leone mettra l'accent sur les questions devant servir à orienter le débat. Parmi les principales tendances nouvelles de la cybermalveillance qui menacent la paix et la sécurité internationales figurent la prolifération des logiciels malveillants, les rançongiciels leurres, les plateformes de location de rançongiciels et les vols de cryptomonnaie. Ces activités exposent les populations civiles à de graves risques et ont des effets dévastateurs sur la sécurité nationale et la stabilité générale de nos pays, ce qui fait peser des risques considérables sur la paix internationale.

Nous sommes vivement préoccupés par l'évolution des tactiques employées dans le cyberespace, qui non seulement alimentent les activités terroristes, mais mettent aussi en péril l'intégrité des systèmes financiers

et des services essentiels. Nous soulignons que le recours croissant aux plateformes de location de rançongiciels et aux vols de cryptomonnaie pour appuyer des activités malveillantes démontre qu'il est urgent de resserrer la coopération et de renforcer les capacités afin de lutter efficacement contre ces menaces. L'intensification récente, tant en termes de fréquence que de portée, des attaques par logiciels rançonneurs, qui prennent pour cible des infrastructures critiques et des services publics essentiels, illustre les répercussions graves que les cybermenaces peuvent avoir sur la sécurité publique et la stabilité politique, et exige une vigilance constante. La Sierra Leone est profondément préoccupée par les conséquences des cybermenaces, notamment le recours à la cybercriminalité pour financer des activités illicites et échapper aux sanctions internationales. Toutes ces conséquences démontrent qu'il est urgent de resserrer la coopération internationale et d'intensifier les efforts de renforcement des capacités pour lutter efficacement contre ces menaces. Nous appelons à une collaboration accrue entre les États Membres afin de renforcer la capacité du Conseil de sécurité de faire face efficacement à la cybermalveillance, en particulier celle qui fait peser des menaces sur les infrastructures critiques, les opérations humanitaires et la protection des civils. Une approche intégrée est indispensable pour maintenir la paix et la sécurité à l'ère numérique.

Nous estimons que l'utilisation malveillante des TIC agit comme un multiplicateur de menaces dans la mesure où elle exacerbe les conflits et les défis existants. La montée des cyberactivités malveillantes visant les infrastructures critiques, notamment les hôpitaux et d'autres systèmes de soins de santé, les services financiers, le secteur de l'énergie, les satellites, les transports et d'autres systèmes d'urgence, souligne la nécessité urgente d'une action mondiale concertée en vue de protéger nos réseaux et systèmes numériques, ainsi que l'importance pour le Conseil de sécurité de se saisir de ces questions et de participer à la gestion et au règlement des conflits qui impliquent des cyberéléments.

Comme nous l'avons déjà entendu, malgré les avantages considérables qu'elle présente, l'IA peut être utilisée comme une arme pour mener des cyberattaques plus complexes et de plus large portée, avec plus de rapidité. Les systèmes autonomes peuvent mener des attaques continues et adaptatives, en apprenant de leur environnement pour exploiter plus efficacement les vulnérabilités. Ces attaques pilotées par l'IA peuvent prendre pour cible les infrastructures critiques, les systèmes financiers et même la vie privée des individus, entraînant des perturbations et des dégâts considérables. Cependant, nous avons également conscience qu'en tirant parti de l'IA à des fins de cyberdéfense, nous pouvons garder une longueur d'avance sur les nouvelles menaces. L'IA peut améliorer la détection des menaces, les délais d'intervention et la gestion des incidents. En investissant dans des technologies défensives fondées sur l'IA, nous pouvons construire une cyberinfrastructure plus résiliente. En investissant dans le renforcement des capacités et le transfert de technologies, nous pouvons améliorer les capacités des pays en développement. La Sierra Leone est d'avis que le Conseil de sécurité peut jouer un rôle central s'agissant de faire face à la nature évolutive des cybermenaces et de promouvoir la paix et la sécurité internationales dans le cadre de contacts étroits avec les comités compétents de l'Assemblée générale et les institutions et organismes spécialisés.

Depuis une dizaine d'années, le Conseil de sécurité est de plus en plus souvent saisi de la question des implications du cyberespace pour la paix et la sécurité internationales. Depuis 2016, les membres du Conseil ont organisé plusieurs réunions selon la formule Arria, au cours desquelles les États ont abordé la question de la cybersécurité en l'associant à des questions telles que la protection des infrastructures critiques, la protection des civils, ainsi que la désinformation et les discours de haine dans le cyberespace.

Aussi la Sierra Leone félicite-t-elle l'Estonie d'avoir organisé le premier débat public de haut niveau sur le sujet durant sa présidence du Conseil en juin 2021. Compte tenu de l'importance croissante accordée par le Conseil de sécurité à la cybersécurité, nous appuyons la proposition d'organiser une séance d'information à intervalles réguliers consacrée à l'évolution des cybermenaces, avec l'éclairage de diverses parties prenantes, afin de garantir une compréhension globale des nouveaux défis et de garder une longueur d'avance sur eux. Nous insistons sur la nécessité d'une coordination, d'une coopération et d'une mobilisation efficaces du Conseil si nous voulons lutter contre les cybermenaces de manière globale.

Nous soulignons que le Conseil de sécurité peut participer à ces efforts dans le cadre de la complémentarité avec d'autres processus engagés par l'ONU concernant l'informatique et les communications, notamment les discussions sur les normes de comportement responsable des États dans l'utilisation des technologies de l'information et des communications, ainsi que le cadre de comportement responsable des États dans le cyberespace, qui a été adopté par consensus, sous les auspices de l'Assemblée générale.

En analysant ces menaces et en élaborant des stratégies d'intervention, avec l'éclairage du système des Nations Unies, du secteur privé, de la société civile et du monde universitaire, le Conseil pourrait rester au fait des dernières évolutions et de leurs conséquences sur la paix et la sécurité internationales.

Compte tenu des liens entre les cybermenaces et d'autres questions dont le Conseil de sécurité est saisi, les États Membres doivent étudier les moyens d'intégrer efficacement les préoccupations liées au numérique ou aux technologies de l'information et des communications dans les travaux actuels du Conseil. La Sierra Leone suggère de tenir compte des préoccupations liées au cyberespace lorsque le Conseil examine diverses questions thématiques, telles que les missions de maintien de la paix, les sanctions imposées par le Conseil, ou la non-prolifération et la lutte contre le terrorisme.

Le renforcement des capacités nationales en matière de cybersécurité et la promotion de la coopération internationale sont des éléments essentiels de cette approche et pourraient également être intégrés dans chacun de ces axes d'action. En intégrant les considérations liées à la cybernétique dans ses travaux, le Conseil peut mieux relever les défis complexes posés par les cybermenaces de manière globale et intégrée.

Pour notre part, la création du Centre national de coordination de la réponse aux incidents de sécurité informatique en Sierra Leone a conduit à la centralisation du mandat visant à traiter toutes les questions de cybersécurité, y compris la riposte aux cyberincidents en Sierra Leone.

Depuis sa création, le Centre a franchi des étapes importantes dans le renforcement de la résilience du pays en matière de cybersécurité grâce à une approche multidimensionnelle du renforcement des capacités et de la collaboration. Parmi les activités importantes, citons les initiatives de renforcement des capacités axées sur la cybersécurité et la criminalité. Le Centre joue un rôle central dans la sensibilisation et la mise en place de programmes de formation à l'intention de diverses parties prenantes, en collaborant avec des partenaires régionaux et de développement pour organiser des formations spécialisées pour le système judiciaire et les services de détection et de répression sur la cybercriminalité et les preuves électroniques, le transfert de connaissances et le partage des meilleures pratiques en matière de cybersécurité et d'enquêtes sur la cybercriminalité. Ces collaborations améliorent la capacité collective de lutter efficacement contre les cybermenaces mondiales en renforçant les capacités nationales.

Je voudrais conclure mon intervention en soulignant, premièrement, et c'est regrettable, le nombre croissant des cybermenaces dirigées de manière éhontée contre nos institutions multilatérales, internationales et judiciaires. À cet égard, la Sierra Leone condamne catégoriquement les attaques visant la Cour pénale internationale. L'une de ces attaques a été décrite par la Cour comme une « attaque ciblée et sophistiquée, ayant pour but l'espionnage, qui peut donc être interprétée comme une tentative sérieuse de saper le mandat de la Cour ». En tant qu'État partie, la Sierra Leone réaffirme son engagement à soutenir et à défendre les principes et les valeurs inscrits dans le Statut de Rome et à préserver son intégrité face à toute ingérence et à toute pression contre la Cour, ses fonctionnaires et les personnes qui coopèrent avec elle.

Deuxièmement, je voudrais réaffirmer la détermination de la Sierra Leone à promouvoir la cybersécurité en tant qu'aspect fondamental de la paix et de la sécurité internationales et à travailler en collaboration au sein du Conseil de sécurité et de la communauté internationale au sens large pour faire face à l'évolution des menaces complexes dans le cyberespace posées par les activités malveillantes.

M. Bendjama (Algérie) (*parle en anglais*) : Je vous remercie, Monsieur le Président, d'avoir organisé cet important débat public sur les risques croissants que les cybermenaces font peser sur la sécurité mondiale. Je remercie également le Secrétaire général et les intervenants de leurs exposés sur l'augmentation inquiétante des cyberactivités nuisibles.

Les attaques par logiciels rançonneurs contre les infrastructures critiques et le vol d'actifs et de données numériques mettent en péril la sûreté publique et la stabilité politique. L'implication d'acteurs gouvernementaux et non gouvernementaux rend la situation encore plus complexe et plus dangereuse. La diffusion d'éléments de désinformation sur les plateformes en ligne alimente la division, la haine, l'intolérance et, à terme, le terrorisme, les fausses informations s'immisçant dans les affaires des États, entravant la coopération et, en fin de compte, menaçant la paix et la sécurité dans le monde.

Les nouvelles technologies, notamment l'intelligence artificielle, rendent les cybermenaces encore plus graves et plus difficiles à combattre. Par conséquent, nous devons relever ces défis, de manière globale et urgente.

Compte tenu de ces réalités, je tiens à souligner les points essentiels suivants.

Premièrement, les principes énoncés dans la Charte des Nations Unies doivent s'appliquer également au cyberespace. Les technologies de l'information et des communications doivent être utilisées conformément à ces principes.

Deuxièmement, nous nous efforçons de garantir un cyberespace ouvert et sécurisé, ce qui est indispensable pour atteindre les objectifs de développement mondiaux du Programme de développement durable à l'horizon 2030. C'est pourquoi nous avons besoin d'un cadre juridiquement contraignant créé au sein de l'ONU.

Troisièmement, nous devons aider les pays en développement à se protéger contre les cybermenaces et à combler la fracture numérique. Le renforcement de leurs capacités est capital pour sécuriser le cyberespace pour tous les pays et doit être une priorité absolue.

Quatrièmement, la communauté internationale doit joindre ses efforts pour lutter contre la diffusion de fausses informations en ligne. Les gouvernements sont des parties intéressées, et les parties intéressées doivent coopérer dans le respect du droit international. La coopération internationale joue un rôle déterminant pour que nous puissions lutter efficacement contre des cybermenaces en constante évolution.

Cinquièmement, nous devons renforcer le cadre juridique pour prévenir et réprimer la cybercriminalité. À cet égard, je voudrais souligner que mon pays joue un rôle actif dans les efforts déployés au niveau international pour lutter contre l'usage des technologies à des fins préjudiciables pour mener des activités criminelles. Ceci est particulièrement évident dans la façon dont l'Algérie dirige 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. Nous espérons que ce comité obtiendra des résultats positifs à sa prochaine session cet été.

Pour terminer, l'Algérie soutient fermement le rôle de l'ONU dans le traitement des questions liées à l'utilisation des technologies de l'information et des communications qui ont une incidence sur la paix et la sécurité internationales. Le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation et l'Assemblée générale sont des cadres essentiels pour mener un débat ouvert sur les cybermenaces. Ils garantissent la participation de tous les Membres à l'élaboration de la riposte mondiale aux problèmes en matière de cybersécurité, et nous réaffirmons notre engagement à soutenir leur travail précieux.

M. Žbogar (Slovénie) (*parle en anglais*) : Je voudrais remercier la République de Corée d'avoir organisé le débat d'aujourd'hui. Je remercie également le Secrétaire général de son exposé, et je tiens à remercier les intervenants de leurs observations et recommandations.

Je voudrais aborder deux questions qui se rapportent au thème du débat d'aujourd'hui.

Premièrement, en ce qui concerne l'évolution des menaces dans le cyberespace, nous sommes d'avis qu'il est essentiel de bien comprendre l'évolution constante des cybermenaces, en particulier dans le contexte de la croissance rapide des technologies émergentes, telles que l'intelligence artificielle, pour discuter des mesures de coopération que la communauté internationale peut prendre en réponse aux cyberactivités malveillantes. À cet égard, nous saluons les travaux en cours du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) créé par l'Assemblée générale, mais nous reconnaissons également qu'un examen plus approfondi de cette question par le Conseil, par exemple en analysant les conclusions du rapport du Secrétaire général sur les cybermenaces (A/77/92), pourrait apporter une contribution complémentaire. Les cyberactivités malveillantes, telles que les attaques par logiciels rançonneurs et les attaques visant des infrastructures civiles critiques, en particulier lorsqu'elles ont un caractère transfrontières, peuvent poser de nouveaux problèmes et exacerber les menaces existantes contre la paix et la sécurité internationales.

Cela m'amène à mon deuxième point, à savoir la prise en compte de l'évolution des menaces dans le cyberespace. Le Conseil a la responsabilité principale du maintien de la paix et de la sécurité internationales. Pour s'acquitter de ses responsabilités conformément à son mandat, le Conseil doit jouer un rôle décisif dans la désescalade des tensions et la promotion de l'application du principe de responsabilité lorsque des cyberactivités malveillantes menacent la paix et la sécurité internationales. Selon nous, les activités qui soutiennent le terrorisme ou la prolifération des armes de destruction massive, qui exacerbent les conflits existants ou visent les infrastructures critiques civiles, constituent une telle menace et justifient donc l'intervention du Conseil. Dans le même ordre d'idées, le Conseil doit s'attaquer aux cyberactivités malveillantes, telles que les campagnes de désinformation, qui incitent à la violence contre les populations civiles, causent des souffrances humanitaires ou perturbent le travail des

organisations humanitaires et des opérations de maintien et de consolidation de la paix.

À une époque marquée par la numérisation croissante des conflits, il est crucial de souligner l'applicabilité du droit international, y compris le droit international humanitaire et le droit international des droits de l'homme, qui doivent être respectés.

Je voudrais conclure en assurant le Conseil de notre détermination à collaborer avec les membres du Conseil et l'ensemble des États Membres de l'ONU pour poursuivre les discussions sur les cybermenaces qui pèsent sur la paix et la sécurité internationales. Nous restons également déterminés à mettre en œuvre des mesures visant à atténuer ces risques, notamment en appliquant les normes existantes en matière de comportement responsable des États dans le cyberespace.

M^me^ Frazier (Malte) (*parle en anglais*) : Je tiens tout d'abord à remercier la République de Corée d'avoir organisé ce débat public sur une question d'actualité extrêmement importante. Je remercie également le Secrétaire général et les intervenants de leurs exposés éclairants.

Les cyberactivités malveillantes posent des problèmes multiformes qui peuvent avoir de graves répercussions sur le maintien de la paix et de la sécurité internationales. Ceux-ci vont des attaques par logiciels rançonneurs contre les institutions gouvernementales, les infrastructures critiques et les services publics essentiels à l'accès non autorisé aux données stockées sous forme électronique et à leur utilisation.

Nous sommes extrêmement préoccupés par les cyberactivités malveillantes qui visent les institutions gouvernementales et les processus démocratiques, souvent dans l'intention directe de compromettre la stabilité et la sécurité et d'éroder la confiance dans les résultats d'élections démocratiques. La dépendance croissante des défenseuses des droits humains et d'autres militantes à l'égard des technologies numériques accroît le risque de harcèlement et d'attaques en ligne. En outre, les droits humains et les libertés fondamentales, y compris la liberté d'expression et de réunion, sont de plus en plus restreints par une surveillance stricte, les coupures d'Internet et la limitation de la bande passante. Dans le même temps, les plateformes numériques sont souvent exploitées pour diffuser de la désinformation, de la mésinformation et des discours de haine, y compris des contenus misogynes, homophobes et radicaux.

Nos efforts collectifs pour promouvoir la stabilité dans ce domaine doivent être ancrés dans les droits humains, en ligne et hors ligne. Les cyberpolitiques doivent tenir compte des conflits, de l'âge et du genre afin de détecter et de prévenir les effets néfastes des menaces en matière de sécurité numérique, telles que la violence fondée sur le genre facilitée par la technologie. Il est essentiel que les femmes participent pleinement et concrètement, sur un pied d'égalité avec les hommes et en toute sécurité à la prise de décisions dans le domaine numérique, en particulier dans les situations de conflit et d'après-conflit.

Nous réaffirmons que le droit international, en particulier la Charte des Nations Unies, s'applique aux activités menées dans le cyberespace, comme l'a reconnu l'Assemblée générale. Dans le même ordre d'idées, le cadre de comportement responsable des États dans le cyberespace fournit des lignes directrices convenues pour les États Membres. Ce cadre doit être respecté par tous les États Membres, et nous sommes favorables à l'élaboration d'un programme d'action pour garantir un dialogue continu et institutionnalisé. En outre, nous appelons tous les États à faire preuve de diligence, à prendre les mesures appropriées conformément aux normes du cadre de comportement responsable des États dans le cyberespace, et à s'abstenir de participer à des cyberactivités malveillantes menées depuis leur territoire ou de les faciliter.

Les cyberacteurs malveillants parrainés par des États exploitent les logiciels rançonneurs et les vols numériques pour générer des revenus illicites. Ces attaques visent notamment des infrastructures critiques, des institutions financières et des sociétés de cryptomonnaies. Les cyberattaques et la criminalité ne connaissent pas de frontières et aucun pays n'est à l'abri. Selon les rapports, pour la seule année 2023, les cyberactivités malveillantes perpétrées par des pirates informatiques parrainés par la République populaire démocratique de Corée ont généré l'équivalent d'un milliard de dollars. Le régime utilise ces revenus pour financer son programme illégal d'armes de destruction massive, qui menace la paix et la sécurité dans la péninsule et au-delà. Ces activités sont solidement étayées dans les rapports du Groupe d'experts du Comité du Conseil de sécurité créé par la résolution 1718 (2006), qui a joué un rôle précieux dans l'enquête sur ces crimes.

Enfin, le Conseil de sécurité peut jouer un rôle important dans l'examen de la question de la cybersécurité. Ses efforts peuvent et doivent être complémentaires de ceux d'autres instances de cybersécurité au sein de l'Assemblée générale, notamment son groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation. Le Conseil peut servir de cadre

puissant pour renforcer les principes convenus et améliorer la qualité des débats ultérieurs. Il doit promouvoir un cyberespace ouvert, sûr, accessible et pacifique. Nous continuerons à soutenir son engagement renouvelé sur ce sujet.

M. Yamazaki (Japon) (*parle en anglais*) : Je vous remercie sincèrement, Monsieur le Président, du leadership dont vous faites preuve en convoquant à point nommé ce débat public important, et je sais gré au Secrétaire général et aux intervenants de leurs précieux éclairages.

D'emblée, le Japon tient à dire qu'il est déterminé à promouvoir un cyberespace libre, équitable et sécurisé. Ces dernières années, nous avons observé une tendance préoccupante à l'augmentation qualitative et quantitative des cyberopérations menées à des fins malveillantes, notamment les attaques par rançongiciel, les dommages causés aux infrastructures critiques, l'ingérence dans les élections démocratiques et le vol de données sensibles. La hausse alarmante des vols de cryptomonnaies est aussi une menace claire et imminente pour la paix et la sécurité internationales, puisqu'elles sont susceptibles de financer des programmes d'armement illicites. En particulier, il est notoire que la Corée du Nord finance ses programmes d'armes de destruction massive et de missiles balistiques en menant des cyberopérations malveillantes, et la communauté internationale doit s'attaquer d'urgence à ces menaces, comme l'a indiqué le Groupe d'experts du Comité créé par la résolution 1718 (2006). En outre, la prolifération des outils de cyberintrusion disponibles dans le commerce, tels que les logiciels espions, suscite de vives inquiétudes au regard de leur incidence sur la sécurité nationale, les droits humains et la paix et la sécurité internationales. Les enjeux n'ont jamais été aussi élevés.

Pour relever ces défis alarmants et garantir un cyberespace libre, équitable et sécurisé, nous devons faire respecter l'état de droit dans le cyberespace en menant des discussions concrètes sur l'application du droit international en vigueur et en mettant en œuvre les normes, règles et principes convenus en matière de comportement responsable des États. Nous devons également accorder une grande importance à l'échange d'informations sur les menaces potentielles existantes, au partage des meilleures pratiques et à la promotion des efforts de renforcement des capacités. Via des dialogues menés à tous les niveaux, nous devons nous employer à favoriser la confiance, à réduire les menaces et, surtout, à réduire le risque d'erreur d'appréciation. Dans le cadre de l'ONU, le Japon continuera de participer constructivement à l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Le Japon estime également que 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, qui est un cadre orienté vers l'action, devra à l'avenir être une instance permanente appuyant l'application des normes, règles et principes convenus en matière de comportement responsable des États.

Dans le même temps, le Japon est tout à fait d'accord pour dire que le Conseil de sécurité, chargé au premier chef du maintien de la paix et de la sécurité, doit jouer un rôle plus important et complémentaire dans le domaine de la cybersécurité. Le Conseil doit suivre de près les cyberincidents graves qui ont de lourdes conséquences pour la paix et la sécurité internationales, notamment ceux qui visent les infrastructures critiques. Des séances d'information régulières au Conseil seraient très utiles pour suivre l'évolution du panorama des menaces dans le domaine du numérique. En outre, il doit remédier aux cybermenaces qui pèsent de plus en plus sur le régime mondial de non-prolifération et de maîtrise des armements, y compris les risques de prolifération incarnés par des acteurs non étatiques.

Pour terminer, le Japon réaffirme son engagement inébranlable à préserver un cyberespace libre, équitable et sécurisé. Le Conseil de sécurité doit rester très vigilant face aux nouveaux risques de sécurité liés au numérique. Nous attendons avec impatience de continuer de débattre des prochaines mesures que le Conseil prendra pour aborder efficacement ce sujet important après le débat d'aujourd'hui tenu à votre initiative, Monsieur le Président.

Dame Barbara Woodward (Royaume-Uni) (*parle en anglais*) : Je remercie M. Cho Tae-yul, Ministre des affaires étrangères de la République de Corée, d'avoir organisé ce débat et d'avoir porté devant le Conseil de sécurité des idées claires sur la manière dont nous pouvons faire avancer nos travaux dans ce domaine. Je remercie également le Secrétaire général et nos intervenants d'aujourd'hui d'avoir expliqué en quoi les cybermenaces peuvent avoir une incidence sur la paix et la sécurité internationales.

J'aborderai trois tendances qui revêtent une importance pour le Royaume-Uni.

Premièrement, comme nous l'avons entendu, les rançongiciels peuvent perturber les fonctions de l'administration publique et la fourniture de services publics vitaux. Cela crée des conditions propices à l'instabilité

lorsque ces attaques surviennent à grande échelle ou sur des périodes prolongées, ce qui, comme le sait le Conseil, peut affecter la paix et la sécurité. N'importe quel État peut être victime d'un rançongiciel. C'est pourquoi une riposte internationale est requise pour asphyxier l'écosystème qui facilite es attaques et pour permettre à tous les États de renforcer leur résilience et leur capacité de réaction. Le Royaume-Uni qui, aux côtés de Singapour, copréside le pilier politique de l'Initiative de lutte contre les rançongiciels, joue un rôle de premier plan à cet égard. Nous exhortons les États à rejoindre cette initiative.

Deuxièmement, à mesure que le recours aux systèmes d'intelligence artificielle (IA) se développe dans nos sociétés, nous devons comprendre comment les cybermenaces vont évoluer, tout en identifiant comment l'IA peut appuyer nos objectifs en matière de cybersécurité. Les acteurs malveillants et irresponsables peuvent exploiter les vulnérabilités des systèmes d'IA pour induire des comportements spécifiques ou manipuler leur prise de décision. Pour maintenir la paix internationale, les systèmes d'IA devront être sécurisés dès leur conception. C'est pourquoi l'an dernier, durant la présidence britannique du Conseil, le Royaume-Uni a organisé le tout premier débat sur l'IA (voir S/PV.9381), et c'est aussi pourquoi nous avons publié, aux côtés des États-Unis et d'un groupe interrégional de 18 États, des lignes directrices pour le développement de systèmes d'IA sécurisés.

Troisièmement, des acteurs malveillants et irresponsables peuvent aussi tirer parti de la croissance du marché des capacités avancées de cyberintrusion, qui rend le panorama des menaces plus imprévisible pour nous tous. Le Royaume-Uni et la France invitent leurs partenaires internationaux à les rejoindre dans le cadre du processus multipartite de Pall Mall, où nous examinons les démarches propres à répondre à cette préoccupation commune.

Dans ce contexte, nous devons continuer de sensibiliser aux cybermenaces. Ainsi, nous nous inquiétons vivement que la République populaire démocratique de Corée recoure aux cyberactivités malveillantes pour obtenir des cryptomonnaies et financer son programme d'armement illégal. C'est pourquoi nous devons redoubler d'efforts pour veiller à une application effective du régime de sanctions imposé à la République populaire démocratique de Corée.

Enfin, les cybermenaces augmentent également les risques de désinformation. C'est là évidemment un écueil majeur pour nos travaux. Il est stupéfiant d'entendre la Russie accuser le Royaume-Uni de mener une guerre de la désinformation alors que sa propre machine de désinformation a été indéniablement mise au jour, y compris ici à l'ONU. Ce n'est pas notre délégation qui a évoqué, dans cette salle et sur Internet, une conspiration impliquant l'utilisation de chauves-souris et de canards comme armes.

Les cybermenaces sont vouées à représenter toujours plus de risques pour la paix et la sécurité internationales, et les gouvernements doivent évoluer pour y répondre efficacement. Dans ce contexte, le Royaume-Uni reste déterminé à respecter le cadre de comportement responsable des États dans le cyberespace et à collaborer avec d'autres pays, via des efforts de renforcement des capacités et en favorisant les partenariats public-privé.

M^me^ Chanda (Suisse) : Je remercie la République de Corée d'avoir organisé ce débat important sur les défis de la cybersécurité. Je remercie également le Secrétaire général, la professeure Nnenna Ifeanyi-Ajufo, et M. Stéphane Duguin, Directeur exécutif du CyberPeace Institute, à Genève, pour leurs contributions.

La Suisse observe deux évolutions déterminantes dans le cyberespace, qui nous préoccupent. D'une part, la numérisation accrue des conflits et le recours à des opérations cyber pendant les conflits armés sont en train de transformer la nature de ceux-ci. D'autre part, l'intensité croissante des attaques par des logiciels de rançon et des cyberattaques parrainées par des États contre des infrastructures critiques est une préoccupation majeure pour la Suisse. L'utilisation de rançongiciels pour extorquer des devises et cryptomonnaies ou encore le ciblage d'infrastructures critiques menacent de paralyser des structures clés de nos sociétés. Ces activités affectent également la capacité de la communauté internationale à atteindre les objectifs de développement durable à cause de la vulnérabilité accrue des États en voie de développement. Elles peuvent poser une menace pour la paix et la sécurité internationales et relèvent donc de la compétence du Conseil.

La note conceptuelle proposée par la République de Corée (S/2024/446, annexe) s'interroge sur le rôle que peut avoir le Conseil par rapport aux menaces qui découlent des activités malveillantes dans le cyberespace. Qu'il me soit permis d'esquisser quelques options à cet égard.

Premièrement, le Conseil devrait régulièrement prendre note des évolutions et des menaces actuelles en termes de cybersécurité. Étant donné les implications multidimensionnelles et la portée géographique de la question, il serait opportun pour le Conseil de tenir une séance d'information régulière. Lors de cette session,

des présentations pourraient être faites par des représentantes et représentants des entités onusiennes, du secteur privé, de la société civile et du monde académique, ainsi que d'autres entités concernées. Cette sensibilisation lui permettrait de prendre des décisions en toute connaissance de cause, notamment sur des dossiers géographiques spécifiques et dans le cadre des opérations de maintien de la paix.

Deuxièmement, le Conseil devrait réaffirmer certains principes reconnus. Nous attachons une importance toute particulière à l'applicabilité du droit international dans le cyberespace, et notamment du droit international humanitaire aux activités dans l'espace cybernétique dans le cadre de conflits armés. Le Conseil devrait également souligner l'importance de la responsabilité des États et de leur devoir de précaution ainsi que reconnaître les 11 normes de comportement responsable des États dans le cyberespace. Ces éléments, complétés par des mesures de confiance et de renforcement des capacités, constituent le cadre pour un comportement responsable des États dans l'utilisation des technologies de l'information et de la communication, qui a été adopté par consensus par l'ensemble des États Membres de l'ONU. Nous soutiendrions un produit du Conseil qui affirmerait ce cadre et contribuerait ainsi au rétablissement de la confiance.

Finalement, l'activité du Conseil doit être complémentaire aux activités d'autres organes. Il ne s'agit pas pour le Conseil de développer des règles de comportement ou des accords. Ceci est l'apanage de l'Assemblée générale et des processus d'experts qu'elle a mandatés. Le Conseil devrait focaliser son attention à développer sa compréhension des risques et à les atténuer, y compris dans des cas de figure concrets.

L'utilisation responsable du cyberespace présente de vastes opportunités pour relever les défis de demain, malgré les risques reconnus. Dans le Nouvel Agenda pour la paix, le Secrétaire général nous encourage à trouver de nouveaux moyens de nous prémunir contre ces nouvelles menaces. Si les négociations du Pacte pour l'avenir nous offrent la possibilité de développer une compréhension commune à cet égard, le Conseil a également un rôle clef à jouer. Le débat de ce jour le confirme.

M. Fu Cong (Chine) (*parle en chinois*) : Je vous remercie, Monsieur le Président, de présider la séance d'aujourd'hui. Je remercie le Secrétaire général Guterres de son exposé et les deux experts de leurs présentations.

Nous sommes actuellement dans une ère numérique sans précédent, marquée par une révolution des technologies de l'information en évolution rapide et des économies numériques et des cyberéconomies en plein essor, et où la communauté internationale connaît une intégration accélérée vers une communauté ayant un avenir commun, dont les membres ont des intérêts étroitement liés et partagent bonne et mauvaise fortune. Dans le même temps, les risques et les défis liés au cyberespace ne cessent de s'aggraver. Les cyberattaques, le cyberespionnage, la cybercriminalité et la désinformation se poursuivent sans relâche. Le cyberterrorisme est devenu un fléau mondial. La militarisation, la polarisation et l'idéologisation du cyberespace s'intensifient, et le fossé numérique entre les pays et les régions se creuse.

Tous les pays ont des possibilités communes et des intérêts communs dans le cyberespace, mais ils sont également confrontés à des défis communs et assument des responsabilités communes. La communauté internationale doit approfondir les échanges, renforcer la confiance mutuelle, coopérer et promouvoir conjointement la gouvernance du cyberespace et l'élaboration de règles internationales en la matière. La Chine voudrait faire les propositions suivantes.

Premièrement, nous devons bâtir un cyberespace plus pacifique et plus sûr. Le cyberespace est profondément intégré au monde réel et constitue un support important du développement de la société humaine, mais il ne doit jamais devenir un nouveau champ de bataille. Le fait qu'un pays désigne le cyberespace comme un domaine d'opérations militaires, met au point des cybercapacités militaires offensives, établit des cyberalliances militaires et fait pression pour la définition de règles d'engagement dans le cyberespace ne fera que saper la confiance mutuelle entre les pays, augmenter le risque de frictions et de conflits dans le cyberespace et fragiliser la paix et la sécurité internationales. Toutes les parties doivent renoncer aux jeux à somme nulle et à la mentalité de la guerre froide, promouvoir une vision commune, globale, coopérative et durable de la sécurité, défendre fermement le caractère pacifique du cyberespace, prévenir efficacement la militarisation et la course aux armements dans le cyberespace, faire face aux menaces à la cybersécurité par le dialogue et la coopération et s'engager à assurer leur propre sécurité sur la base de la sécurité commune.

Deuxièmement, nous devons bâtir un cyberespace plus inclusif et plus prospère. Les économies numériques et les cyberéconomies constituent désormais un moteur important de la croissance économique mondiale. Tous

les pays doivent donc adopter des politiques plus actives, plus ouvertes, plus coordonnées et plus inclusives pour promouvoir l'application et la popularisation des technologies de l'information et de la communication (TIC) et garantir l'ouverture, la stabilité et la sécurité des chaînes industrielles des TIC afin de permettre à un plus grand nombre de pays et de personnes de profiter des dividendes de l'Internet. Les pays développés doivent aider les pays en développement à promouvoir un développement numérique, propulsé par Internet et intelligent et à améliorer leurs capacités de prévention des risques et de réaction aux situations d'urgence, et garantir un accès équitable aux ressources clefs telles que les technologies de cyberinfrastructure et la puissance de calcul, afin de réduire au minimum la fracture numérique et de réaliser les objectifs de développement durables, énoncés dans le Programme de développement durable à l'horizon 2030. La pratique consistant à former des cliques selon des lignes idéologiques, à élargir le concept de sécurité nationale, à ériger un rideau de fer numérique et à rechercher le monopole et la domination technologiques, même en interférant ouvertement avec le développement économique et technologique d'autres pays et en le réprimant, ne fera qu'entraver les efforts de la communauté internationale pour promouvoir la gouvernance du cyberespace.

Troisièmement, nous devons bâtir un cyberespace plus équitable et plus ordonné. Il est essentiel d'élaborer des règles internationales concernant le cyberespace acceptables par tous pour maintenir durablement la paix et la stabilité dans le cyberespace. Toutes les parties doivent respecter scrupuleusement les buts et principes énoncés dans la Charte des Nations Unies, en particulier les principes d'égalité souveraine, de non-ingérence dans les affaires intérieures, de non-recours à la menace ou à l'emploi de la force et de règlement pacifique des différends, et respecter et mettre en œuvre le cadre des Nations Unies pour le comportement responsable des États dans le cyberespace. Dans le même temps, toutes les parties doivent toujours respecter le rôle de l'ONU, qui est le canal principal à cet égard, et sur la base d'une participation égale et large, traduire le consensus international de longue date en normes juridiquement contraignantes de comportement dans le cyberespace. Les solutions constructives proposées par la Chine, telles que l'initiative mondiale pour la gouvernance de l'intelligence artificielle et l'initiative mondiale pour la sécurité des données, peuvent servir de modèles pour l'élaboration de règles futures relatives au cyberespace.

Quatrièmement, nous devons bâtir un cyberspace plus égalitaire et plus inclusif. La diversité est une caractéristique fondamentale du monde et un moteur du progrès humain. Internet relie tous les pays, tous les peuples et toutes les civilisations comme jamais auparavant et, naturellement, il doit devenir une plateforme importante pour l'ensemble de l'humanité afin de mettre en valeur les diverses cultures et de promouvoir le développement et l'héritage des civilisations. Nous devons exploiter pleinement les TIC, intensifier les échanges en ligne dans le cadre du dialogue, encourager la compréhension mutuelle et l'amitié entre les peuples de tous les pays, promouvoir la tolérance et la coexistence entre les différentes civilisations et mieux promouvoir les valeurs communes de l'humanité. Nous devons être vigilants face à la pratique d'un petit nombre de pays qui cherchent à imposer leurs propres valeurs comme des valeurs universelles et qui s'ingèrent même dans les affaires intérieures d'autres pays, venant perturber leur développement et leur stabilité. Nous devons nous opposer résolument à l'utilisation du cyberespace pour propager l'extrémisme, le terrorisme, la désinformation et les discours de haine.

La Chine est à la fois témoin et bénéficiaire du développement d'Internet. Aujourd'hui, elle compte près de 1,1 milliard d'utilisateurs. Nous avons construit la cyberinfrastructure la plus vaste et la plus avancée technologiquement du monde et nous avons mis en place un système solide de politiques pour la gouvernance du cyberespace. Ces dernières années, la Chine a activement renforcé sa communication et son partage d'expérience avec les pays du Sud en matière de politique ; promu une coopération pratique en matière de renforcement des capacités dans des domaines tels que les infrastructures, la technologie, l'application de la loi et la réponse aux situations d'urgence ; participé activement aux processus de cybersécurité dans des cadres tels que le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), le Groupe des 20, l'Association de coopération économique Asie-Pacifique, le groupe Brésil, Russie, Inde, Chine et Afrique du Sud, l'Organisation de coopération de Shanghai et le Forum régional de l'Association des nations de l'Asie du Sud-Est, entre autres ; et apporté une contribution importante à la promotion de la gouvernance mondiale du cyberespace.

La révolution de l'information, qui est une tendance de notre époque, progresse à grands pas. Le cyberespace évoque l'espoir infini de l'humanité en un avenir radieux. La Chine est prête à travailler avec la communauté internationale pour construire un cyberespace plus pacifique, plus sûr, plus ouvert, plus coopératif et plus ordonné, et à œuvrer de concert pour bâtir une communauté avec un avenir commun dans le cyberespace.

M. De La Gasca (Équateur) (*parle en espagnol*) : Je tiens à saluer la présence de M. Cho Tae-yul, Ministre des affaires étrangères de la République de Corée. Je remercie également le Secrétaire général António Guterres des informations fournies et les intervenants, M. Stéphane Duguin et M^me^ Nnenna Ifeanyi-Ajufo, de leurs exposés.

Dans un monde de plus en plus interconnecté et interdépendant, la cybersécurité est un défi mondial qui exige une réponse coordonnée et coopérative de la part de l'ensemble de la communauté internationale.

L'utilisation malveillante des technologies de l'information et de la communication (TIC) agit commun un multiplicateur des menaces à la paix et la sécurité, notamment dans les domaines suivants.

Premièrement, les TIC peuvent être utilisées pour nuire aux infrastructures critiques, telles que les systèmes de santé, les services financiers et les réseaux énergétiques, qui sont essentielles au fonctionnement des sociétés.

Deuxièmement, elles peuvent servir à diffuser la désinformation et les discours de haine, ce qui a pour effet de polariser davantage les sociétés et d'alimenter les conflits.

Troisièmement, elles peuvent être employées pour soutenir des activités terroristes et financer les activités illicites d'acteurs étatiques et non étatiques.

Face à ces défis, le Conseil de sécurité ne doit pas rester à la traîne en ce qui concerne l'évolution des cybermenaces, car celles-ci sont liées à plusieurs points de l'ordre du jour du Conseil, notamment la non-prolifération et la lutte contre le terrorisme. À cet égard, le Conseil de sécurité doit envisager la possibilité d'intégrer des éléments liés à la cybersécurité dans ses produits, en fonction des besoins de chaque dossier. Le renforcement de la communication stratégique dans les opérations de paix et les missions politiques spéciales en est un exemple.

La promotion d'un cyberespace sûr, ouvert et pacifique exige des normes de comportement responsable dans l'utilisation des TIC. En outre, le développement du droit international dans ce domaine doit s'accompagner d'un renforcement des capacités, en particulier dans les pays en situation de conflit, qui sont les plus vulnérables face à l'utilisation abusive des TIC. Le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) progresse dans ce domaine. Le produit de ses travaux pourrait servir de guide pour les travaux du Conseil.

Je conclus en rappelant la nécessité de préserver et de promouvoir une utilisation responsable du cyberespace afin de garantir sa stabilité et sa sécurité et de réduire ainsi le risque substantiel qu'il fait peser sur les nations.

M. de Rivière (France) : Je remercie le Secrétaire général, M. Duguin et M^me^ Ifeanyi-Ajufo pour leurs interventions et je vous remercie, Monsieur le Président, d'avoir organisé ce débat.

L'essor des technologies de l'information et de la communication contribue au progrès et à la réalisation des objectifs de développement durable. Il pose néanmoins des défis majeurs pour notre sécurité collective. Dans des sociétés fortement dépendantes de ces technologies, les activités cyber malveillantes n'ont cessé de croître en fréquence, en gravité et en sophistication. Elles peuvent exploiter des vulnérabilités nombreuses et utiliser des vecteurs de plus en plus divers, accessibles désormais à de multiples acteurs. Les outils et services d'intrusion se diffusent de façon incontrôlée sur les marchés, et leur usage irresponsable contribue à l'accroissement des menaces cyber.

Les cyberattaques peuvent constituer en elles-mêmes des menaces pour la paix et la sécurité internationales, par leur impact sur des infrastructures critiques et les risques d'escalade qu'elles induisent. Les attaques par rançongiciels, dont les autorités françaises ont constaté une hausse de 30 % en 2023, peuvent ainsi toucher des secteurs essentiels comme celui de l'énergie, déstabiliser les économies, voire perturber le fonctionnement des institutions gouvernementales. Des cyberattaques sont désormais conduites dans le contexte de conflits armés, comme l'ont illustré les attaques menées par la Russie contre le réseau satellitaire Viasat dans les premières heures de son invasion illégale de l'Ukraine.

Les activités cyber malveillantes peuvent également alimenter d'autres menaces pour la paix et la sécurité internationales, comme celle de la prolifération. Le dernier rapport du Groupe d'experts du Comité du Conseil de sécurité créé par la résolution 1718 (2006) (S/2024/215) indiquait que les programmes illégaux d'armes de destruction massive du régime nord-coréen seraient financés à hauteur de 40 % par des moyens cyber illicites, tels que les rançongiciels ou les vols de cryptomonnaie.

L'Organisation des Nations Unies et le Conseil de sécurité, dans l'exercice de son mandat, disposent cependant des moyens de mettre en œuvre une réponse concertée à ces menaces. Rappelons d'abord que le cyberespace n'est pas un Far West, ni un vide normatif. Le

droit international y est pleinement applicable, y compris la Charte des Nations Unies, le droit international humanitaire et le droit international des droits de l'homme. Des normes de comportement étatique responsable ont été définies par consensus, afin de promouvoir la coopération, de favoriser la prévention des conflits et d'améliorer la stabilité dans le cyberespace.

La France soutient les travaux menés dans le cadre de la Première Commission de l'Assemblée générale afin de poursuivre le développement de ce cadre normatif. Afin d'en soutenir la mise en œuvre, la France a proposé une structure pour un futur mécanisme ambitieux de programme d'action cyber. Le Conseil de sécurité doit placer le respect du cadre normatif de comportement responsable des États dans le cyberespace au cœur de ses travaux sur les menaces cyber et encourager les États à mettre en œuvre leurs engagements pour concourir à la sécurité et à la stabilité du cyberespace.

Au-delà, le Conseil de sécurité doit continuer ses efforts pour intégrer les enjeux cyber dans les différentes dimensions de son mandat. Il est indispensable que le Conseil reçoive régulièrement des présentations d'experts sur l'évolution des menaces cyber et leurs implications pour la paix et la sécurité internationales. Le débat d'aujourd'hui constitue un exemple précieux à cet égard.

Le Conseil doit continuer à prêter attention à l'usage de moyens cyber pour contourner les régimes de sanctions. Les activités cyber malveillantes menées par le régime nord-coréen pour financer ses programmes d'armes de destruction massive méritent à ce titre une attention continue. La France reste mobilisée pour que le Conseil, malgré la non-reconduction du Groupe d'experts du Comité 1718, continue à suivre avec vigilance les violations de ses résolutions en ce domaine.

Le Président (*parle en anglais*) : Je donne maintenant la parole à S. E. M. Mamadou Tangara, Ministre des affaires étrangères, de la coopération internationale et des Gambiens de l'étranger de la République de Gambie.

M. Tangara (Gambie) (*parle en anglais*) : Je voudrais tout d'abord remercier les intervenants de leurs exposés éclairants et féliciter la République de Corée d'avoir organisé le présent débat.

Nous sommes à la croisée des chemins. L'ère numérique a tissé une toile de connexions, de possibilités et de progrès. Pourtant, au sein même de cette trame se cache un mal grandissant qui menace la paix et la sécurité internationales. La menace que représente la cybercriminalité, qui ne cesse d'évoluer, n'est pas seulement une question de gains financiers ou de données volées. La nouvelle vague de cybermenaces remet directement en cause la paix et la sécurité internationales, et exige une attention urgente de notre part. À cet égard, nous remercions la République de Corée d'avoir attiré notre attention sur une nouvelle facette des travaux du Conseil de sécurité, en vue d'échanger des vues de fond sur le thème « Maintien de la paix et de la sécurité internationales : faire face à l'évolution des menaces dans le cyberespace ». En tant qu'organe chargé de maintenir la paix et la sécurité internationales, le Conseil de sécurité ne peut se permettre de rester silencieux, et nous le félicitons des efforts continus qu'il déploie pour tirer la sonnette d'alarme sur cette question importante qui nous concerne tous. Nous avons besoin d'une approche globale pour faire face à cette menace en constante évolution.

À cet égard, je voudrais formuler les trois suggestions suivantes pour appuyer les efforts conjoints que nous déployons en vue d'endiguer les cybermenaces qui pèsent sur la paix et la sécurité internationales.

Premièrement, le Conseil de sécurité doit devenir un champion des normes exemplaires de comportement responsable des États dans le cyberespace, et nous pouvons y parvenir en menant régulièrement des actions de sensibilisation pour favoriser les discussions sur la cybersécurité en vue d'amplifier la portée des travaux menés par l'Assemblée générale dans ce domaine, ainsi qu'en collaborant avec les États Membres pour traduire ces normes en actes, et en encourageant le renforcement des capacités et l'échange d'informations afin de mettre un frein aux activités malveillantes.

Deuxièmement, le Conseil de sécurité peut renforcer l'application du principe de responsabilité en ce qui concerne les cybermenaces pesant sur la sécurité en encourageant les États Membres à améliorer leurs cybercapacités afin d'identifier les acteurs malveillants et de joindre leurs forces pour lutter contre l'impunité.

Troisièmement, le Conseil de sécurité peut tirer parti des compétences spécialisées des entités des Nations Unies, telles que le Bureau des affaires de désarmement et le Bureau de lutte contre le terrorisme, pour faire face de manière adéquate aux menaces pesant sur la viabilité de la paix, de la sécurité et de la démocratie internationales. La collaboration avec ces entités peut également déboucher sur une coordination permettant d'éviter les chevauchements et d'adopter une approche intégrée, adaptée à l'objectif visé.

Ces actions, entreprises dans le cadre du mandat du Conseil, contribueront non seulement à promouvoir la paix et la sécurité internationales, mais aussi à renforcer les efforts existants en renforçant la sensibilisation, en promouvant l'application du principe de responsabilité et en encourageant une collaboration efficace entre les États et les institutions internationales concernées. Le Conseil de sécurité est dès lors bien placé pour jouer un rôle de premier plan dans l'édification d'un cyberespace plus sûr et plus stable pour tous.

Nous devons élever le débat et intégrer régulièrement les cybermenaces dans nos discussions sur les conflits régionaux et les questions thématiques. Cela amplifie la portée des travaux menés au sein des instances de l'Assemblée générale qui traitent des cybernormes. Nous devons également encourager les États Membres à traduire ces normes en mesures concrètes. Il s'agit notamment de renforcer les capacités de cyberdéfense, de promouvoir l'échange d'informations et de mettre un frein aux activités malveillantes.

Pour terminer, je tiens à féliciter une fois de plus la République de Corée pour cette initiative louable, qui donne aux États Membres l'occasion de participer à ce débat très important et d'actualité sur une question d'intérêt commun. Le Conseil de sécurité joue un rôle central s'agissant d'apporter un appui indispensable pour atténuer et éliminer les cybermenaces qui pèsent sur la paix et la sécurité internationales.

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

M. Lindner (Allemagne) (*parle en anglais*) : L'Allemagne remercie la République de Corée d'avoir pris l'initiative de porter les questions de cybersécurité à l'attention du Conseil de sécurité. Je tiens également à remercier le Secrétaire général et les intervenants de leurs contributions éclairantes.

La communauté internationale est exposée à un nombre de plus en plus important de cyberactivités malveillantes, qu'elles soient commanditées par des États ou le fait d'acteurs privés. Ces activités ont de lourdes répercussions sur le maintien de la paix et de la sécurité internationales. Des attaques graves menées par des cybercriminels, notamment des attaques par rançongiciels, ont montré que de telles attaques pouvaient mettre en péril la stabilité des institutions étatiques. Elles ont eu des conséquences sur des sociétés entières.

Depuis peu, on assiste à l'émergence, sur le théâtre des conflits internationaux, de groupes d'hacktivistes qui prennent pour cible des infrastructures critiques de premier plan. Cette tendance affaiblit la confiance dans la prestation des services publics et sème la peur parmi les civils. La coopération croissante d'un certain nombre d'acteurs étatiques avec des sociétés informatiques privées, des groupes d'hacktivistes et des cybercriminels contribue à exacerber les risques. Toutes ces tendances ont pour effet de multiplier les menaces, étant donné que le cyberdomaine étend les champs de bataille traditionnels jusqu'au domaine civil.

Face à l'évolution spectaculaire des menaces, l'Allemagne propose quatre domaines dans lesquels le Conseil de sécurité se doit d'agir.

Premièrement, nous considérons que le Conseil de sécurité a un rôle important à jouer dans l'évaluation des menaces, à la fois en vertu de l'Article 34 de la Charte des Nations Unies, qui donne au Conseil le pouvoir d'enquêter sur toute situation qui pourrait entraîner un désaccord entre nations ou engendrer un différend, et plus généralement dans le sens où le Conseil doit examiner et analyser plus en profondeur les risques provenant des cyberattaques qui pèsent sur la paix et la sécurité internationales.

Deuxièmement, le Conseil de sécurité a aussi un rôle important à jouer dans le règlement des différends, étant donné que la Charte des Nations Unies est pleinement applicable au cyberespace.

Troisièmement, nous estimons que le Conseil de sécurité peut jouer un rôle majeur dans l'instauration d'un climat de confiance et l'établissement de normes. En intégrant les cyberconflits internationaux dans ses travaux, en enquêtant sur les situations de cyberconflit ou en facilitant le règlement pacifique de ces situations, le Conseil contribuera à l'élaboration d'un cadre évolutif régissant le comportement responsable des États dans le cyberespace. Cette démarche doit se fonder sur le droit international et être complétée par des normes volontaires établies par l'ONU et des mesures de confiance.

Enfin, l'Allemagne se félicite des efforts déployés par le Conseil de sécurité pour tenir compte des cybermenaces dans ses travaux. Il s'agit notamment de protéger l'ONU contre les cyberattaques malveillantes, en particulier sur le terrain, par exemple dans le cadre des opérations de maintien de la paix.

Pour terminer, je voudrais souligner que l'Allemagne continuera de contribuer au débat international sur cette question importante. Pour ne citer qu'un exemple, nous avons lancé l'année dernière un dialogue mondial consacré au cyberespace dans les situations de conflit.

Il vise spécifiquement à traiter les risques croissants que l'utilisation d'outils cybernétiques dans les conflits internationaux fait peser sur les civils, à sensibiliser l'opinion et à proposer des solutions pour atténuer ces risques. Le prochain dialogue sera organisé ici à New York, à la German House, le 8 juillet, en coopération avec le Japon, le Sénégal et le Comité international de la Croix-Rouge.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant des Émirats arabes unis.

M. Sharaf (Émirats arabes unis) (*parle en anglais*) : Je remercie S. E. M. Cho Tae-yul, Ministre sud-coréen des affaires étrangères, de présider ce débat public, et je félicite la République de Corée de la compétence avec laquelle elle dirige les travaux du Conseil de sécurité ce mois-ci. Je remercie également le Secrétaire général et les autres intervenants de leurs contributions éclairantes.

Comme nous l'avons entendu aujourd'hui, les menaces qui pèsent sur le cyberespace évoluent rapidement. Des outils et des techniques cybernétiques malveillants, tels que les rançongiciels, l'hameçonnage et les attaques par déni de service, sont utilisés pour attaquer les réseaux des secteurs public et privé, menaçant ainsi les infrastructures critiques et la sécurité publique. Cette situation est d'autant plus préoccupante que nos pays, y compris les Émirats arabes unis, sont en pleine transformation numérique, ce qui entraîne une forte dépendance à l'égard des systèmes en ligne sécurisés. Les établissements d'enseignement sont également menacés, puisque des acteurs malveillants prennent pour cible l'infrastructure numérique du secteur de l'éducation et les informations précieuses qu'elle renferme. En outre, l'utilisation malveillante des technologies de l'information et des communications, y compris, mais sans s'y limiter, les nouvelles technologies fondées sur l'intelligence artificielle (IA), agit comme un multiplicateur de menaces dans les conflits existants.

En tant que centre mondial de la technologie et de l'innovation, les Émirats arabes unis ont créé, en 2020, le Conseil de la cybersécurité. Le Conseil de la cybersécurité vise à réaliser une transformation numérique plus sûre et à améliorer la cybersécurité dans le pays pour tous les secteurs susceptibles de subir des attaques. Nous sommes déterminés à renforcer les capacités et à partager les informations avec nos partenaires, ainsi qu'à promouvoir la conception responsable des technologies et à utiliser l'intelligence artificielle à bon escient pour lutter contre la propagation et l'amplification des discours de haine, de la mésinformation et de la désinformation. Conformément à cet engagement, nous avons organisé, avec l'Albanie, en décembre 2023, une réunion selon la formule Arria afin de nous pencher sur ces défis.

Dans cette optique, je voudrais proposer quatre points à prendre en considération.

Premièrement, le droit international doit guider l'utilisation des cybertechnologies. La Charte des Nations Unies, la souveraineté, la non-ingérence dans les affaires intérieures des États, la responsabilité des États et le droit des conflits armés doivent être respectés, y compris les normes de comportement responsable des États dans le cyberespace établies par l'ONU. Pour combler les lacunes normatives, il faut qu'il y ait toujours une convergence de vues sur la manière de faire respecter et de préserver le droit international dans le domaine cybernétique.

Deuxièmement, les Émirats arabes unis sont favorables à l'intégration des préoccupations liées au numérique dans les travaux du Conseil relatifs à la paix et à la sécurité internationales. Il faudrait notamment mentionner plus régulièrement les préoccupations, les tendances et les évolutions liées au numérique dans les séances d'information, les déclarations et les questions prioritaires, ainsi que dans les dossiers portant sur tel ou tel pays ou les questions thématiques. Ainsi, la résolution 2341 (2017) reconnaît la nécessité de protéger les infrastructures critiques contre les attaques terroristes, y compris de garantir la cybersécurité, ce qui souligne la nécessité de mieux faire face au large éventail de cybermenaces qui vont de pair avec la numérisation et le cyberespace.

Troisièmement, le Conseil doit envisager d'organiser une séance d'information annuelle sur les menaces technologiques émergentes et leurs conséquences sur la paix et la sécurité internationales. En outre, la publication d'un rapport annuel sur la cybersécurité par le Secrétaire général fournirait une analyse complète des cybermenaces au niveau mondial et des recommandations pour renforcer la coopération internationale. Le rapport doit également inclure une analyse des questions de genre afin de mieux faire face aux cybermenaces qui visent les femmes et les filles.

Quatrièmement, il est essentiel de favoriser des partenariats public-privé solides pour tirer parti des connaissances et des ressources afin de lutter efficacement contre les cybermenaces. Les Émirats arabes unis sont déterminés à collaborer avec le secteur privé pour mettre au point des outils de cybersécurité robustes et renforcer les capacités nationales et internationales, tout

en aidant le secteur privé à concevoir des solutions sûres et responsables.

L'exploitation des cybertechnologies revêt la plus haute importance pour notre avenir, mais la vigilance face aux risques qu'elles présentent est capitale. La coopération internationale et le renforcement des capacités sont d'une importance vitale pour la résilience de la sécurité mondiale. Les Émirats arabes unis continueront à promouvoir un comportement responsable dans le cyberespace et à veiller à ce que ce comportement reflète nos aspirations collectives à la paix et à la sécurité.

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

M^me^ Melbārde (Lettonie) (*parle en anglais*) : La Lettonie voudrait exprimer sa gratitude à la République de Corée pour l'organisation de ce débat public de haut niveau du Conseil de sécurité. Nous tenons également à remercier de leurs exposés éclairants le Secrétaire général, ainsi que les intervenants du CyberPeace Institute et de l'Université Beckett de Leeds.

L'utilisation des technologies numériques et la dépendance à leur égard se sont considérablement accrues depuis que les questions liées à la cybersécurité ont été inscrites pour la première fois à l'ordre du jour de l'ONU, il y a plus de 20 ans. Aujourd'hui, le cyberespace est au cœur du développement économique et social mondial. Tout en offrant de vastes possibilités de progrès, l'expansion du cyberespace est également associée à des risques et à des défis croissants. Ces dernières années, nous avons observé plusieurs tendances négatives en ce qui concerne la paix et la sécurité internationales. Il y a de plus en plus de cas où des infrastructures critiques, notamment des infrastructures d'information critiques, sont la cible de cyberattaques qui peuvent avoir des conséquences catastrophiques dans le monde réel. En outre, nous constatons que les cyberattaques font désormais partie intégrante de l'agression à grande échelle de la Russie contre l'Ukraine.

Les cybermenaces sont souvent associées à d'autres actes hostiles, tels que la propagation de la désinformation et de la mésinformation et l'utilisation malveillante de l'intelligence artificielle et d'autres technologies émergentes. La cybercriminalité est également omniprésente, les sommes versées à des logiciels rançonneurs ayant atteint un niveau record en 2023. Ces évolutions ont des répercussions sur la paix et la sécurité mondiales. La communauté mondiale doit coordonner sa réponse, et le Conseil de sécurité a un rôle à jouer conformément à son mandat.

Par conséquent, la Lettonie estime que les menaces et les défis liés au cyberespace méritent d'être examinés régulièrement par le Conseil. Ces discussions pourraient s'appuyer sur un rapport périodique du Secrétaire général. Accroître l'attention portée par le Conseil à la cybersécurité pourrait également faciliter l'intégration des aspects liés à la cybernétique dans d'autres mandats thématiques, tels que le maintien de la paix et les femmes et la paix et la sécurité. Le Conseil doit également envisager de renforcer sa capacité de riposter aux cyberattaques de grande ampleur susceptibles d'avoir des conséquences sur la sécurité internationale.

Il est évident qu'il n'est pas possible de renforcer le rôle du Conseil en ce qui concerne les questions de cybersécurité du jour au lendemain. Il s'agit d'une entreprise progressive, et les séances telles que celle d'aujourd'hui jouent un rôle essentiel dans la facilitation de ce processus. Il est également clair que les travaux du Conseil ne doivent pas remplacer ceux déjà effectués dans d'autres enceintes de l'ONU relevant de l'Assemblée générale. Bien au contraire, le Conseil doit renforcer les accords conclus dans ces instances, en particulier l'applicabilité du droit international dans son intégralité au cyberespace. Par ailleurs, beaucoup reste à faire collectivement pour mettre en œuvre le cadre de comportement responsable des États dans le cyberespace. En attendant la mise en place d'un mécanisme permanent de l'ONU chargé de la cybersécurité, connu sous le nom 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, nous pensons qu'il est possible de créer de nouvelles synergies entre le Conseil et l'Assemblée générale dans ce domaine.

Pour terminer, je voudrais souligner la détermination de la Lettonie à continuer d'appuyer les efforts déployés au sein de l'ONU pour faire face aux menaces et aux défis croissants en matière de cybersécurité. Nous participons activement aux discussions sur ce sujet au sein des instances de l'Assemblée générale, et nous continuerons également à plaider en faveur d'un rôle plus important pour le Conseil.

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

M^me^ Rizk (Égypte) (*parle en anglais*) : L'Égypte attache une grande importance aux aspects des technologies de l'information et des communications liés à la sécurité internationale et demande instamment que l'ONU joue un rôle central et de premier plan dans la promotion et l'élaboration de règles et de principes pour l'utilisation

des technologies de l'information et des communications par les États, dans le cadre d'un processus inclusif et équitable auquel participent tous les États.

Un certain nombre d'États développent des capacités en matière de technologies de l'information et des communications en vue d'éventuelles utilisations malveillantes et à des fins militaires offensives. L'utilisation des technologies de l'information et des communications dans les futurs conflits entre États devient une réalité, et le risque d'attaques préjudiciables menées à l'aide de ces technologies contre les infrastructures critiques est à la fois réel et sérieux. Cette nouvelle course aux armements a des répercussions considérables sur la paix, la sécurité et la stabilité internationales, d'autant plus que la frontière entre les armes classiques et non classiques est de plus en plus ténue.

En outre, les technologies pertinentes mises au point par les États sont transférées, copiées et reproduites par des terroristes et des criminels. L'utilisation malveillante des technologies de l'information et des communications par des organisations terroristes et criminelles constitue une menace grave pour la paix et la sécurité internationales, compte tenu en particulier des défis liés à l'attribution. En vertu du droit international et de la Charte des Nations Unies, tous les États Membres doivent s'abstenir de poser, sciemment ou intentionnellement, tout acte qui endommagerait ou compromettrait l'utilisation et le fonctionnement des infrastructures critiques d'autres États, ainsi que de toute ingérence dans leurs affaires intérieures. Il ne fait aucun doute que les aspects des technologies de l'information et des communications liés à la sécurité internationale sont devenus trop importants et stratégiques pour qu'il n'y ait pas de règles contraignantes claires au niveau international en la matière. Un processus inclusif au sein du système des Nations Unies est le meilleur moyen de conclure des normes équitables, globales et efficaces dans ce domaine.

L'ONU a déjà pris certaines mesures pour mettre en place un cadre normatif qui complète les principes du droit international. Avec l'adoption par consensus de deux rapports d'activité annuels du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), créé en application de la résolution 75/240 de l'Assemblée générale, et d'autres rapports consensuels dans le cadre de processus liés à l'ONU, celle-ci a déjà mis en place les premiers éléments d'un cadre pour la prévention des conflits et la stabilité dans le cyberespace.

L'Assemblée générale a invité les États Membres à s'inspirer, dans leur utilisation des technologies de l'information et des télécommunications, du cadre cumulatif et évolutif élaboré aux fins du comportement responsable des États dans le cyberespace, qui figure dans les rapports consécutifs des groupes d'experts gouvernementaux relevant de la Première Commission. Toutefois, la mise en œuvre de ces normes reste, au mieux, assez limitée en raison de leur caractère facultatif et de l'absence d'un mécanisme de suivi.

Tout en reconnaissant les progrès accomplis par le groupe de travail à composition non limitée créé en vertu de la résolution 75/240 de l'Assemblée générale sur différents aspects de son mandat, il est important que le groupe jette les bases d'un mécanisme futur orienté vers l'action, à voie unique, fondé sur le consensus et inclusif, sous les auspices de l'ONU. Il doit s'appuyer sur les résultats obtenus dans le cadre des processus liés à l'ONU et mettre l'accent sur la mise en œuvre des textes qui ont été adoptés, y compris le cadre de comportement responsable des États dans le cyberespace, tout en développant ce cadre et en promouvant la coopération internationale avec les pays en développement et une assistance en leur faveur.

Les processus inclusifs au sein de l'ONU, principalement sous les auspices de l'Assemblée générale, sont le moyen le plus efficace d'établir des normes équitables, globales et efficaces dans ce domaine. Pour sa part, le Conseil de sécurité est encouragé à prendre en compte les possibilités offertes par les technologies émergentes lorsqu'il examine des questions telles que le maintien de la paix et la lutte contre le terrorisme. Néanmoins, le Conseil ne doit pas être utilisé comme un organe législatif qui tente de fixer des normes et des règles au nom des États Membres de l'ONU sur des questions qui exigent des processus inclusifs et transparents.

Les recommandations qui ont été approuvées par consensus à l'Assemblée générale peuvent constituer la base de règles politiquement ou juridiquement contraignantes, d'autant plus qu'elles découlent des principes consacrés par le droit international et la Charte des Nations Unies. Si nous estimons que le droit international et les principes énoncés dans la Charte des Nations Unies s'appliquent à tous les domaines, y compris le cyberespace, nous pensons également qu'il est urgent d'identifier les obligations spécifiques qui rendent le comportement des États dans le cyberespace conforme au droit international et aux buts et principes énoncés dans la Charte des Nations Unies.

Dans un monde toujours plus connecté, la solidité de tout régime international de cybersécurité dépendra de celle de son maillon le plus faible. Heureusement, il existe un consensus quant à la nécessité d'intensifier et de renforcer les efforts de renforcement des capacités afin de prévenir les attaques potentielles contre les infrastructures critiques et de développer les capacités et les compétences techniques nécessaires dans les pays en développement. L'ONU doit prendre la tête d'efforts coordonnés pour fournir l'assistance nécessaire aux pays en développement.

Pour terminer, les technologies de l'information et des communications présentent des possibilités et des défis considérables, et nous soulignons qu'il est urgent de définir et d'élaborer des règles de comportement responsable des États pour renforcer la stabilité et la sécurité dans l'environnement numérique mondial et empêcher que le cyberespace ne devienne un nouveau théâtre de conflit et de la course aux armements.

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 à la représentante de l'Ukraine.

M^me^ Hayovyshyn (Ukraine) (*parle en anglais*) : Nous remercions la présidence coréenne du Conseil de sécurité d'avoir organisé ce débat public de haut niveau. Nous remercions également le Secrétaire général et les autres intervenants de leurs déclarations.

L'Ukraine s'associe à la déclaration qui sera prononcée au nom de l'Union européenne et voudrait ajouter quelques observations à titre national.

Nous sommes convaincus que le Conseil de sécurité joue un rôle important dans la lutte contre les menaces qui pèsent sur la paix et la sécurité internationales, y compris dans le cyberespace. Les cybermenaces continuent d'évoluer et sont devenues plus problématiques que jamais. Les logiciels rançonneurs représentent un risque de plus en plus courant et important pour les gouvernements, les entreprises et les particuliers. En outre, nous assistons à une augmentation du nombre de cyberopérations malveillantes visant les infrastructures critiques et les infrastructures d'information critiques, notamment le secteur de l'énergie, les services publics et les processus électoraux. Certains acteurs étatiques continuent de saper l'ordre international fondé sur des règles et le cadre de comportement responsable des États dans le cyberespace en menant des cyberactivités malveillantes.

À cet égard, la République populaire démocratique de Corée se livre à des activités de cyberespionnage et de vol de cryptomonnaies dans le but de poursuivre le développement de ses programmes d'armes nucléaires et d'armes de destruction massive, en violation des résolutions pertinentes du Conseil de sécurité. Récemment, le groupe de cyberespionnage russe APT28 a mené des cyberattaques contre plusieurs États membres de l'Union européenne.

L'Ukraine est confrontée à l'agression de la Russie, y compris dans le cyberespace. Depuis le début de la guerre, les cyberattaques russes sont de plus en plus sophistiquées et visent les institutions gouvernementales et les organismes de sécurité, les entreprises et les institutions financières. Les cybercriminels moscovites commettent des attaques par hameçonnage, des actes de cyberespionnage et des attaques contre des infrastructures critiques, tout en diffusant de la désinformation et de la propagande.

Pour prévenir, contrer et atténuer efficacement les cybermenaces, l'Ukraine coopère activement avec des partenaires internationaux pour développer des cybercapacités efficaces, ce qui est fondamental si elle veut pouvoir exercer son droit de légitime défense dans le cyberespace. En outre, l'Ukraine a également commencé à enquêter sur les cyberattaques en tant que crimes de guerre et à en poursuivre les auteurs.

Les États doivent s'acquitter de leurs obligations et engagements internationaux, y compris pour garantir l'utilisation en toute sécurité des technologies de l'information et des communications. Comme nous l'avons réaffirmé ici à l'ONU, le droit international, y compris la Charte des Nations Unies, est applicable dans le cyberdomaine. Par conséquent, tous les acteurs étatiques qui se comportent d'une manière contraire au cadre convenu doivent être tenus de rendre des comptes.

Pour terminer, nous encourageons les États Membres à poursuivre leurs efforts collectifs pour renforcer et mettre en œuvre le cadre normatif de comportement responsable des États dans le cyberespace, sensibiliser le public et échanger leurs pratiques optimales afin de faire face aux menaces actuelles et émergentes dans le cyberdomaine.

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

M. Tammsaar (Estonie) (*parle en anglais*) : Nous nous félicitons de l'échange de vues d'aujourd'hui et nous remercions les intervenants, en particulier le Secrétaire général, de leurs précieuses observations.

L'Estonie s'associe à la déclaration qui sera faite par la représentante de l'Union européenne. Je souhaite faire quelques observations à titre national.

Nous ne pouvons ignorer la sophistication croissante des cyberincidents malveillants orchestrés par des acteurs étatiques et non étatiques et les dommages qu'ils causent. Sachant que les cyberattaques visent des cibles de premier plan, telles que les infrastructures critiques, les institutions financières et les processus démocratiques, et compte tenu de leur caractère transfrontières et des capacités croissantes, elles peuvent provoquer des dommages de plus en plus importants. Par conséquent, la cybersécurité fait clairement partie des préoccupations nationales et internationales en matière de sécurité, et la prévention et l'atténuation de ces menaces sont une priorité commune.

L'agression de la Russie contre l'Ukraine a mis en évidence le lien entre les cyberopérations et les actes de guerre cinétique. Nous avons vu comment les infrastructures critiques ukrainiennes sont prises pour cible par la Russie, en violation du droit international humanitaire. Les agissements de la Russie illustrent la nécessité de se concentrer sur une approche globale de la défense nationale et de la sécurité intérieure. Afin de renforcer la préparation et la résistance de l'Ukraine face aux cyberattaques, l'Estonie soutient activement l'Ukraine dans le domaine numérique au niveau bilatéral, ainsi que par le biais du Mécanisme de Tallinn et de la Coalition pour les technologies de l'information.

Nous sommes également très préoccupés par les dernières nouvelles en provenance de Pyongyang selon lesquelles la coopération militaire entre la République populaire démocratique de Corée et la Russie aurait été renforcée, en violation flagrante des résolutions pertinentes du Conseil de sécurité. L'Estonie condamne fermement les cyberactivités malveillantes menées par la République populaire démocratique de Corée, qui visent à alimenter le programme d'armement de la République populaire démocratique de Corée, à déstabiliser la sécurité régionale et à menacer la paix mondiale.

Le cadre de comportement responsable des États dans le cyberespace adopté par l'ONU s'appuie sur le droit international en vigueur. Le droit international, en particulier la Charte des Nations Unies, le droit de la responsabilité des États, le droit international des droits de l'homme et le droit international humanitaire, s'applique pleinement aux cyberopérations. Nous devons travailler de concert pour faire respecter le droit international et veiller à ce qu'il soit également appliqué dans le cyberespace. Pour contribuer à la mise en œuvre du cadre de comportement responsable des États dans le cyberespace, l'Estonie préconise la mise en place d'un programme d'action inclusif et orienté vers l'action en tant que structure permanente unique après la conclusion des activités de l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation en 2025.

Un environnement numérique ouvert, sûr, stable, accessible et pacifique, ne peut être considéré comme acquis et est indissociable du monde physique. L'agression de la Russie contre l'Ukraine a mis en évidence la nature intégrée des cyberattaques et de la guerre cinétique, et nous pensons qu'il s'agit d'un schéma qui sera répliqué dans les conflits futurs. Le Conseil de sécurité a donc un rôle important à jouer en servant d'instance où partager les informations sur les cybermenaces existantes et à venir et où sensibiliser aux implications stratégiques de la cybersécurité, ce que l'Estonie avait déjà souligné au cours de son mandat au Conseil.

En guise de conclusion, c'est pour cette raison que l'Estonie félicite la République de Corée d'avoir fait en sorte que cette discussion se tienne de l'instance idoine qu'est le Conseil. Des discussions publiques comme celle-ci sur la cybersécurité seront cruciales pour appuyer le renforcement de la résilience nationale, régionale et mondiale face aux cyberattaques, en contribuant à la prévention et à l'atténuation des risques de cyberconflit.

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

M. Kulhánek (République tchèque) (*parle en anglais*) : Avant toute chose, je tiens à remercier la République de Corée d'avoir organisé ce débat public très pertinent. Nous nous félicitons du débat convoqué aujourd'hui sur le rôle du Conseil de sécurité dans le domaine de la cybersécurité, en particulier concernant l'application du cadre convenu s'agissant d'un comportement responsable des États dans le cyberespace.

Il va sans dire que nous partageons bon nombre des préoccupations et avertissements qui ont été exprimés ici aujourd'hui. Les attaques contre les infrastructures critiques, le cyberespionnage, les attaques par rançongiciel contre des institutions tant publiques que privées, notamment dans le secteur de la santé, les vols de cryptomonnaies et les efforts en vue d'accéder de manière durable

à des systèmes industriels critiques, non seulement à des fins d'espionnage et de vol de propriété intellectuelle, mais aussi pour être en mesure de les commander de manière ouvertement hostile, nous inquiètent particulièrement. Le recours croissant au numérique dans les conflits armés, qui a des effets néfastes sur les civils, est alarmant. Ces actes irresponsables mettent en péril la paix et la sécurité internationales, dont le Conseil de sécurité assume la responsabilité. De la même manière, le cyberespace sert de plus en plus à diffuser de la désinformation, à exacerber les conflits sociaux et même à encourager des actes terroristes. Le Conseil, ainsi que les instances compétentes de l'ONU et les autres organisations internationales saisies de la question du numérique doivent intensifier leurs efforts pour trouver des moyens efficaces de lutter contre les activités moins visiblement malveillantes dans le cyberespace. Ils doivent également s'efforcer de sensibiliser à l'ampleur réelle de ces menaces et faciliter les activités qui favorisent une résilience accrue.

En mai, la Tchéquie, en coordination avec l'Allemagne et d'autres États, a condamné publiquement les activités du groupe APT28, commandé par l'État russe, qui menait de longue date une campagne de cyberespionnage dans les pays européens et s'en était pris aux institutions du Gouvernement tchèque. Ces activités contreviennent aux normes de l'ONU en matière de comportement responsable des États dans le cyberespace. Nous continuerons de nous y attaquer avec énergie, en collaboration avec nos partenaires et dans le respect de nos obligations internationales.

La Tchéquie adhère pleinement à un ordre international fondé sur le droit international et promouvant un environnement numérique ouvert, sûr, stable, accessible et pacifique. Nous réaffirmons notre appui à la création d'un mécanisme permanent, à voie unique, inclusif et orienté vers l'action, sous l'égide de l'ONU, lorsque prendra fin, en 2025, l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Nous sommes convaincus que 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 pourrait remplir cette fonction.

Enfin, je tiens à redire que mon pays reste déterminé à participer activement à ce qui doit être un partenariat véritablement mondial si nous voulons venir à bout des menaces qui pèsent et pèseront sur la cybersécurité. Tout le monde, littéralement, devra être sur le pont. Nous avons déjà entamé des discussions approfondies avec un certain nombre de pays d'Afrique, de la région Indopacifique et d'Amérique latine afin de recenser les menaces mouvantes et de muscler notre riposte collective. Ainsi, fin avril, la Tchéquie a organisé à Bogota un séminaire sur les défis auxquels nous sommes déjà confrontés s'agissant des activités criminelles dans le cyberespace. Nous remercions les experts venus de la Colombie, du Costa Rica, de la République dominicaine, de l'Équateur, d'El Salvador, du Guatemala, du Honduras et du Panama pour participer à cet événement, qui nous ont fait part de leurs précieux éclairages.

Je vous remercie à nouveau, Monsieur le Président, de m'avoir donné l'occasion de partager les vues de mon pays sur ce sujet important.

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

M^me^ Samson (*parle en anglais*) : J'ai l'honneur de prendre la parole au nom de l'Union européenne et de ses États membres. La Macédoine du Nord, le Monténégro, l'Albanie, l'Ukraine, la République de Moldova, la Bosnie-Herzégovine et la Géorgie, pays candidats, ainsi que l'Andorre, s'associent à la présente déclaration.

Je vous remercie, Monsieur le Président, d'avoir organisé ce débat public de haut niveau. L'Union européenne se félicite de ce débat qui nous permet d'échanger des points de vue sur l'évolution du panorama des cybermenaces, et sur ce qu'elle signifie pour le maintien de la paix et de la sécurité internationales.

Les déclarations qui viennent d'être faites ont couvert un large éventail de menaces émergentes et mouvantes, allant des attaques par déni de service, à faible impact, aux attaques contre les infrastructures critiques, en passant par les cyberopérations à grande échelle. Nous ajoutons à ces préoccupations les répercussions transfrontières que pourrait avoir une cyberactivité malveillante. Nous constatons également que la frontière est floue entre les activités criminelles et les attaques pour lesquelles des États font appel à des cybercriminels, ce qui rend d'autant plus ardue la tâche déjà difficile d'en attribuer les responsabilités. Nous devons nous engager de concert à renforcer notre panoplie d'outils favorisant la résilience collective, et nous nous réjouissons que d'autres délégations partagent leurs éclairages et leurs expériences.

L'Union européenne et ses États membres s'alarment du nombre, de la sophistication et de l'ampleur des cyberactivités malveillantes qui s'en prennent aux institutions gouvernementales et aux processus démocratiques. Le mois dernier, l'Allemagne a partagé son évaluation

selon laquelle le groupe de cyberespionnage APT28, associé à la Russie, avait piraté les comptes de courrier électronique du Parti social-démocrate allemand. Les institutions, organismes et entités publics de certains États membres de l'Union européenne, notamment la République tchèque, la Pologne, la Lituanie, la Slovaquie et la Suède, avaient déjà été pris pour cible par ce même acteur malveillant. Ces activités malfaisantes doivent cesser.

Les normes de l'ONU relatives à un comportement responsable des États dans le cyberespace fournissent des orientations à cet égard. Les principaux engagements sont simples : le droit international s'applique dans le cyberespace ; les États sont censés respecter des normes volontaires de comportement ; ils doivent empêcher l'utilisation abusive du cyberespace sur leur territoire ; et des mesures de confiance concrètes doivent être prises pour contribuer à réduire le risque d'escalade et de conflit liés à des cyberincidents. Pour l'Union européenne, il est crucial de se concentrer sur le développement et la mise en œuvre du cadre convenu pour un comportement responsable des États dans le cyberespace si nous voulons nous acquitter de notre responsabilité partagée, conformément à notre intérêt commun, et protéger tous les États contre les risques de cyberactivité malveillante. Les États peuvent réaliser des progrès sensibles en précisant l'application du droit international en vigueur et en discutant de la mise en œuvre et du respect des normes en place en matière de comportement responsable. Pour que le cadre convenu en matière de comportement responsable des États soit suivi d'effet, nous devons le respecter ensemble. Cela renforce l'importance de mettre en place, sous les auspices de l'ONU, un mécanisme permanent, inclusif et orienté vers l'action. Nous sommes donc favorables à la création d'un 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 nous espérons que nous conviendrons de ses modalités dès cet été.

Nous nous réjouissons à l'idée de faire progresser les discussions sur ce sujet important et nous saluons les initiatives tels que celle-ci, qui cherchent à mettre en exergue le rôle important que, dans l'exercice du mandat que lui a confié la Charte des Nations Unies, le Conseil de sécurité joue s'agissant de remédier aux menaces à la paix et à la sécurité internationales, en mettant en évidence les menaces internationales singulières et spécifiques qui se font jour dans le cyberespace. Nous espérons également continuer d'envisager comment les travaux futurs du Conseil peuvent compléter efficacement d'autres processus pertinents des Nations Unies à cet égard.

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

M. Lagdameo (Philippines) (*parle en anglais*) : Les Philippines saisissent cette occasion pour insister à nouveau sur l'importance cruciale de la lutte contre les menaces que les technologies de l'information et de la communication (TIC) font peser sur la sécurité internationale. Les progrès rapides des technologies numériques posent de nouveaux défis qui nécessitent une action immédiate et concertée. À cet égard, nous souhaitons mettre l'accent sur trois points essentiels : les tendances en matière de menaces liées aux TIC, les conséquences des cybermenaces sur la paix et la sécurité internationales et les cyberattaques en tant que multiplicateur de menace.

Premièrement, en ce qui concerne les tendances des menaces liées aux TIC, l'augmentation des appels automatisés s'appuyant sur l'intelligence artificielle (IA) et utilisés à des fins frauduleuses, la prolifération des hypertrucages et de la mésinformation et les attaques par rançongiciels présentent des risques considérables et des défis complexes. Des stratégies globales sont essentielles pour contrer ces menaces sophistiquées. L'utilisation malveillante de l'IA dans le cyberespace présente des risques importants. Nous devons donner la priorité à l'évaluation de ces menaces afin d'élaborer des politiques de cybersécurité robustes et de garantir le déploiement en toute sécurité des technologies de l'IA.

Deuxièmement, en ce qui concerne les conséquences des cybermenaces sur la paix et la sécurité nationales, les Philippines ont fait l'expérience directe des effets dévastateurs des cyberattaques sur la sécurité nationale et la confiance du public. Des incidents récents, tels que la défiguration de sites Web gouvernementaux, les atteintes à la sécurité des données visant des institutions critiques et le vol à grande échelle d'informations personnelles, soulignent la nécessité urgente de renforcer les mesures de cybersécurité. Les cyberattaques peuvent perturber les services essentiels, porter atteinte à la confiance dans les institutions et avoir des conséquences socioéconomiques considérables. Nous sommes également particulièrement préoccupés par les activités malveillantes liées aux TIC qui visent à s'immiscer dans les affaires intérieures des États. Nous constatons une augmentation des signalements d'utilisation malveillante par les États de campagnes d'information clandestines facilitées par les TIC afin d'influer sur les processus, les systèmes et la stabilité générale d'autres États. Ces activités minent la confiance, comportent un risque d'escalade et peuvent menacer la paix et la sécurité

internationales. Autre considération alarmante, ces capacités technologiques sophistiquées sont à la disposition d'acteurs non étatiques qui peuvent les utiliser de manière malveillante à des fins commerciales et pour échapper à toute responsabilité.

Troisièmement, en ce qui concerne l'effet multiplicateur des cyberattaques en termes de menaces, les activités criminelles dans le cyberespace exacerbent les défis existants pour la paix et la sécurité internationales. Les Philippines ont pu constater que les cyberattaques peuvent constituer un important multiplicateur de menace, compliquant les efforts de maintien de la paix et de la stabilité. La nature transnationale du cyberespace signifie qu'aucun État n'est à l'abri et que notre sécurité collective est aussi forte que son maillon le plus faible. Compte tenu des risques graves que font peser les cybermenaces, les Philippines soulignent le rôle central que doit jouer le Conseil de sécurité dans la lutte contre ces menaces. Si les discussions en cours au sein du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) sont utiles, il est également impératif que le Conseil de sécurité continue de participer à l'élaboration du Programme mondial cybersécurité.

À cet égard, les Philippines sont favorables à ce que le Conseil prenne les mesures collectives suivantes pour lutter contre les cybermenaces, comme cela a été évoqué au cours de la réunion organisée selon la formule Arria sur la cybersécurité qui s'est tenue en avril : premièrement, renforcer le cadre normatif convenu concernant le comportement responsable des États dans le cyberespace ; deuxièmement, organiser une séance annuelle pour examiner le paysage des menaces liées aux TIC et, à cet égard, demander au Secrétaire général de préparer un rapport annuel sur les tendances afin d'éclairer les discussions des États Membres ; et troisièmement, diriger la collecte d'informations ou l'étude de menaces ou d'incidents spécifiques à des fins d'orientation et de référence pour les États Membres.

Les Philippines réaffirment leur engagement à renforcer la cyberrésilience et à promouvoir un comportement responsable dans le cyberespace. Nous appelons à la poursuite de la coopération, des efforts de renforcement des capacités et des mécanismes de soutien, y compris un fonds d'affectation spéciale régulier pour aider les pays en développement à faire face aux cybermenaces. Nous comptons sur les partenariats et les transferts de technologie pour nous aider à réduire la fracture numérique et à renforcer nos cyberdéfenses.

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

M. Nasir (Indonésie) (*parle en anglais*) : L'Indonésie remercie la République de Corée d'avoir organisé cette importante séance. Nous remercions également le Secrétaire général et les intervenants de leurs exposés.

Les menaces dans le cyberespace sont devenues un danger réel et bien présent pour la paix et la sécurité nationales et internationales. Nous sommes de plus en plus exposés à de nouvelles menaces provenant de technologies nouvelles et en évolution rapide. Ce n'est que par une réponse coordonnée et des cadres juridiques solides que la communauté internationale pourra renforcer la cyberrésilience et atténuer ces risques de manière efficace.

Dans ce cadre, qu'il me soit permis de souligner les points suivants.

Premièrement, nous devons donner la priorité à l'atténuation du coût humain des cyberattaques qui visent les infrastructures critiques. Nous devons veiller à ce que le cyberespace soit préservé en tant que domaine libre de tout conflit et non en tant qu'arène de conflit. Si les progrès de l'intelligence artificielle (IA), y compris l'IA générative et l'apprentissage automatique, peuvent profiter à l'humanité, ils peuvent aussi être destructeurs et faciliter les cyberattaques, entraînant des conséquences négatives considérables pour la population mondiale. Il est donc essentiel de protéger les infrastructures critiques dans le cadre des efforts que nous déployons pour éviter que des cyberacteurs malveillants et des États irresponsables ne causent des dommages importants.

Deuxièmement, les synergies et la cohérence au sein du système des Nations Unies dans les domaines de la cybersécurité, des technologies de l'information et de la communication (TIC) et de la paix et de la sécurité internationales sont essentielles. Si le Conseil de sécurité a le mandat fondamental de maintenir la paix et la sécurité internationales, d'autres organes des Nations Unies ont des mandats tout aussi cruciaux pour travailler sur les questions de sécurité numérique, de sécurité des TIC et de cybersécurité. Il est important que le Conseil de sécurité établisse des paramètres et des mécanismes qui peuvent l'aider à favoriser la collaboration et les synergies, nous permettant ainsi de mieux comprendre les risques que les cybermenaces font peser sur la paix et la sécurité internationales. C'est pourquoi l'Indonésie réaffirme son attachement aux travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) ainsi qu'à d'autres processus

entrepris dans ce domaine, notamment dans le cadre du processus du Sommet de l'avenir.

Troisièmement, nous devons améliorer la cybersécurité mondiale en renforçant la coopération régionale. La coopération avec les organisations régionales est nécessaire, car elles jouent un rôle important en contribuant à une approche solide et globale de la cybersécurité. Dans notre région, l'Association des nations de l'Asie du Sud-Est (ASEAN) joue un rôle déterminant dans la création de cadres et d'initiatives, notamment par l'intermédiaire du Forum régional de l'ASEAN, afin d'améliorer la résilience régionale face aux cybermenaces. Mettre à profit ce savoir-faire des organisations régionales peut en effet fournir des informations précieuses et favoriser un effort international plus global.

Enfin, nous devons combler le fossé technologique pour améliorer la cyberrésilience. Le manque de capacités en matière de cybersécurité constitue une difficulté de taille pour les pays en développement, les rendant vulnérables face à l'intensification des menaces et compromettant leur stabilité. Des mesures de coopération à tous les niveaux, y compris avec les acteurs concernés du secteur privé, sont indispensables pour améliorer la stabilité dans le cyberespace, notamment par le biais du renforcement des capacités, de l'assistance technique et du transfert de technologies. Ce n'est qu'en unissant nos efforts que nous pourrons créer un cyberespace sûr qui favorisera la paix et la stabilité dans le monde.

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

M. Seah (Singapour) (*parle en anglais*) : Nous remercions la République de Corée d'avoir organisé la séance d'aujourd'hui sur cette question importante.

Depuis le premier débat public du Conseil de sécurité sur la cybersécurité, qui a eu lieu en juin 2021 (voir S/2021/621), le paysage des cybermenaces a continué d'évoluer à un rythme inquiétant. Dans ce contexte, la coopération internationale au sein de l'ONU est vitale et indispensable pour lutter contre la nature mondiale et transfrontière des cybermenaces. À cet égard, l'Assemblée générale et le Conseil de sécurité doivent œuvrer de concert pour renforcer l'adhésion au cadre normatif du comportement responsable des États, fondé sur l'application du droit international et le respect des principes consacrés par la Charte des Nations Unies. En tant que petit État, Singapour a toujours appuyé un système multilatéral fondé sur l'état de droit. Notre approche n'est pas différente en ce qui concerne la cybersécurité, qui est d'une importance vitale pour de nombreux petits États et États en développement. Singapour croit fermement à l'importance de l'ONU, qui constitue un cadre de premier plan pour discuter de l'élaboration et de l'application des règles, normes et principes de comportement responsable des États qui régissent le cyberespace.

Singapour a l'honneur de présider depuis 2021 le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Le groupe de travail à composition non limitée s'appuie sur plus de deux décennies d'efforts à l'ONU, qui ont abouti à un cadre cumulatif et évolutif de comportement responsable des États dans le cyberespace, lequel a été approuvé par tous les États Membres. Il est encourageant de constater que le groupe de travail à composition non limitée a accompli des progrès satisfaisants au cours des trois dernières années en renforçant le cadre normatif de comportement responsable des États dans le cyberespace.

Le groupe de travail à composition non limitée constitue également une mesure de confiance précieuse en soi. Outre les accords qui figurent dans les deux rapports d'activité annuels du groupe de travail à composition non limitée adoptés par consensus en juillet 2022 (voir A/77/275) et en juillet 2023 (voir A/78/265), respectivement, le groupe de travail à composition non limitée a joué un rôle de premier plan dans l'élaboration et la mise en œuvre d'initiatives concrètes orientées vers l'action qui ont un rôle important à jouer dans le renforcement de la paix et de la sécurité internationales dans le cyberespace, en particulier sous la forme du répertoire mondial d'interlocuteurs, qui a été officiellement lancé le 9 mai. Toujours en mai, le groupe de travail à composition non limitée a organisé une réunion ministérielle fructueuse sur les questions de fond liées au renforcement des capacités en matière de sécurité du numérique. Le message fondamental qui est ressorti de cette réunion est qu'il est urgent de renforcer les capacités pour aider de nombreux petits pays et pays en développement à atteindre la cyberrésilience. Tout aussi important, il a été largement reconnu que le renforcement des capacités pouvait être un moyen important de consolider la confiance entre les États.

Dans vos questions visant à orienter le débat, Monsieur le Président, vous avez demandé comment les cybermenaces sont liées à d'autres questions dont est saisi le Conseil de sécurité et quel rôle le Conseil de sécurité peut jouer pour relever les défis concernant la paix et la sécurité internationales que pose le cyberespace. Compte tenu des travaux en cours à l'Assemblée générale, il est important que le Conseil de sécurité évite de faire double

emploi avec les travaux déjà réalisés dans le cadre d'autres processus. Dans le même temps, nous devons reconnaître que le Conseil de sécurité a un mandat clair pour aborder les questions relatives au maintien de la paix et de la sécurité internationales. Nous ne pouvons pas exclure la possibilité qu'un cyberincident crée des malentendus entre États et conduise à une escalade, voire à un conflit, ce qui constituerait une atteinte à la paix et à la sécurité internationales. Nous ne pouvons donc pas exclure la possibilité que le Conseil de sécurité joue un rôle dans le cadre des responsabilités qui lui incombent en vertu de la Charte en matière de maintien de le paix et de la sécurité internationales.

Le Conseil doit donc garder l'esprit ouvert au sujet de ce qui constitue une menace pour la paix et la sécurité internationales et agir en étant conscient que les cybermenaces peuvent avoir des conséquences physiques et réelles. À cet égard, nous sommes réceptifs à l'idée que le Conseil de sécurité continue d'organiser des débats publics comme celui d'aujourd'hui afin d'échanger des informations et d'améliorer la compréhension de ces questions par les États Membres. Les discussions au sein du Conseil peuvent contribuer à éclairer les travaux de l'Assemblée générale, notamment dans les domaines du renforcement des capacités et de la confiance, et à renforcer le cadre de comportement responsable des États dans le cyberespace, notamment en examinant la meilleure façon d'appliquer les règles, les normes et les principes aux cybermenaces existantes et potentielles.

Je termine en soulignant la nécessité d'améliorer la coopération internationale afin de renforcer notre résilience collective dans le cyberespace. La promotion d'une plus grande coopération entre le Conseil de sécurité et l'Assemblée générale sur les questions de paix et de sécurité internationales et une collaboration soutenue, holistique et synergique permettront à la communauté internationale de préserver plus efficacement la paix et la sécurité internationales dans le domaine du cyberespace. Singapour est prête à collaborer avec tous les États Membres pour atteindre cet objectif.

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

M^me^ Chan Valverde (Costa Rica) (*parle en espagnol*) : Je remercie la République de Corée d'avoir organisé le présent débat public.

Il y a deux ans, le Costa Rica a été victime d'attaques de logiciels rançonneurs à grande échelle. Nous ressentons toujours les effets des perturbations qui ont touché notre système de santé, notre sécurité sociale, notre secteur financier et d'autres secteurs critiques.

À cet égard, le Costa Rica voudrait faire trois observations aujourd'hui.

Premièrement, le Costa Rica est convaincu que le programme de protection des civils doit être étendu aux cyberactivités qui touchent les populations civiles en période de conflit armé. Les États doivent se rallier au consensus croissant selon lequel les données civiles bénéficient de la même protection au regard du droit international humanitaire que tous les autres biens de caractère civil, et les cyberopérations qui neutralisent ou entravent le fonctionnement des systèmes civils sont interdites par le droit international humanitaire. Les États doivent également s'abstenir d'impliquer des civils dans les cyberactivités militaires, car cela pourrait les mettre en danger.

Deuxièmement, le Costa Rica estime qu'il est temps d'actualiser le programme pour les femmes et la paix et la sécurité afin d'aborder la question de la sécurité des femmes dans la sphère numérique. Le Costa Rica demande aux membres du Conseil de sécurité d'envisager l'adoption d'une nouvelle résolution qui prévoirait des mesures visant à protéger les femmes et les filles contre la violence, les abus et l'exploitation en ligne, en particulier dans les situations de conflit et d'après-conflit. Les considérations relatives à la sécurité numérique doivent également être intégrées systématiquement dans tous les nouveaux mandats, initiatives et objectifs liés à ce programme.

Troisièmement, tous les États, qu'ils soient ou non membres du Conseil, sont tenus de renforcer l'état de droit international dans le cyberespace. Le Costa Rica est fier de faire partie d'un groupe croissant d'États qui ont adopté des positions nationales sur l'application du droit international dans le cyberespace. Ces prises de position s'appuient sur le consensus mondial selon lequel le droit international, y compris le droit international humanitaire et le droit international des droits de l'homme, s'applique à l'utilisation par les États des technologies de l'information et des communications et est essentiel au maintien de la paix et de la stabilité. Nous encourageons d'autres États à élaborer de tels documents de position et nous saluons les ressources existantes pour le renforcement des capacités juridiques, telles que le Cyber Law Toolkit, qui peuvent guider les efforts dans ce domaine.

Vu que nos sociétés sont de plus en plus vulnérables face aux menaces cybernétiques et numériques, le Costa

Rica exhorte le Conseil à prendre en compte ces préoccupations dans ses travaux et à le faire d'une manière qui renforce le respect du droit international en temps de paix comme en période de conflit armé.

Le Président (*parle en anglais*) : Il reste un certain nombre d'orateurs et d'oratrices inscrits sur la liste pour la présente séance. Je me propose, avec l'assentiment des membres du Conseil, de suspendre la séance jusqu'à 15 heures.

La séance est suspendue à 13 h 10.