Nations Unies S/PV.9039

Conseil de sécurité

Soixante-dix-septième année

Provisoire

9039e séance
Lundi 23 mai 2022, à 10 heures
New York

Présidente :	Mme Thomas-Greenfield	(États-Unis d'Amérique)
Membres :	Albanie	M. Hoxha
	Brésil	M. de Oliveira Marques
	Chine	M. Zhang Jun
	Émirats arabes unis	Mme Nusseibeh
	Fédération de Russie	M. Nebenzia
	France	M. de Rivière
	Gabon	M. Biang
	Ghana	M. Agyeman
	Inde	M. Tirumurti
	Irlande	M. Flynn
	Kenya	M. Kiboino
	Mexique	M. Gómez Robledo Verduzco
	Norvège	Mme Juul
	Royaume-Uni de Grande-Bretagne et d'Irlande du Nord	M. Roscoe

Ordre du jour

Maintien de la paix et de la sécurité internationales

Technologie et sécurité

La séance est ouverte à 10 h 5.

Adoption de l'ordre du jour

L'ordre du jour est adopté.

Maintien de la paix et de la sécurité internationales

Technologie et sécurité

La Présidente (*parle en anglais*) : Conformément à l'article 39 du règlement intérieur provisoire du Conseil, j'invite les personnalités ci-après, appelées à présenter un exposé, à participer à la présente séance : M^me^ Rosemary DiCarlo, Secrétaire générale adjointe aux affaires politiques et à la consolidation de la paix ; M^me^ Nanjala Nyabola, Directrice d'Advox, projet de Global Voices dédié aux droits numériques ; et M. Dirk Druet, chargé d'enseignement au Centre d'études sur la paix et la sécurité internationale de l'Université McGill et chercheur non résident auprès de l'International Peace Institute.

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

Je donne la parole à M^me^ DiCarlo.

M^me^ DiCarlo (*parle en anglais*) : Les technologies numériques ont profondément transformé toutes les facettes de nos sociétés. Elles regorgent de possibilités pour le développement durable, l'enseignement et l'inclusion. Les médias sociaux, par exemple, ont transformé la promotion des droits humains et de l'action humanitaire en permettant, dans le monde entier, une mobilisation rapide et efficace autour de questions exigeant une attention urgente. Ils ont également créé de nouvelles possibilités pour nos activités consacrées à la paix et la sécurité. Grâce aux progrès technologiques, nous sommes désormais mieux à même de détecter les crises, de prépositionner nos dotations humanitaires et de concevoir des programmes de consolidation de la paix fondés sur des données.

Nous exploitons les technologies numériques dans nos activités de prévention des conflits et de rétablissement et de consolidation de la paix. Je citerai quelques exemples.

Les outils numériques enrichissent nos capacités de collecte d'informations et d'alerte rapide. Au Yémen, la Mission des Nations Unies en appui à l'Accord sur Hodeïda a utilisé divers outils issus des technologies de la cartographie, des systèmes d'information géographique et des satellites pour améliorer sa surveillance du cessez-le-feu dans la province. Les outils numériques nous permettent d'être mieux préparés à comprendre et analyser les crises susceptibles d'avoir une dimension numérique et à y réagir, ainsi qu'à remédier aux risques numériques. Ainsi, nous avons œuvré en collaboration avec nos partenaires pour mettre en place une plateforme d'apprentissage en ligne consacrée à la gestion des risques numériques.

Les nouvelles technologies peuvent être un atout à l'appui des processus politiques, en particulier s'agissant de promouvoir l'inclusion. Dans le cadre de diverses négociations de paix, nous avons tiré parti des dialogues numériques assistés par intelligence artificielle pour atteindre des milliers d'interlocuteurs et connaître leurs vues et leurs priorités. Cela a été particulièrement utile pour nouer le contact avec des groupes traditionnellement exclus, notamment les femmes.

En Libye, la Mission d'appui des Nations Unies a organisé cinq dialogues numériques, auxquels plus de 1 000 personnes ont participé à chaque fois. Cet effort a renforcé la légitimité du processus, puisque les diverses communautés se sont rendu compte qu'elles pouvaient faire entendre leur voix. Au Yémen, des consultations numériques ont permis à l'Envoyé spécial de mobiliser des centaines de femmes de différentes provinces, ce qui a fourni de précieux éclairages sur les incidences que la guerre a sur elles.

Le recours aux technologies numériques peut également améliorer la sûreté et la sécurité de nos soldats de la paix et des personnels civils sur le terrain. Le lancement de la Stratégie pour la transformation numérique du maintien de la paix des Nations Unies a franchi une étape essentielle dans ce sens, et favorise une mise en œuvre plus efficace des mandats en augmentant les capacités d'alerte rapide.

Enfin, grâce à ces outils, nous sommes en mesure de visualiser les informations et de transmettre au Conseil de sécurité des analyses riches en données pour appuyer sa prise de décision. Nous avons récemment fait au Conseil de sécurité une présentation en réalité virtuelle sur la Colombie qui a montré que nous disposons de nouveaux moyens de lui faire connaître notre travail sur le terrain.

Les avantages des technologies numériques pour le maintien de la paix et de la sécurité internationales sont multiples. Cela étant, les progrès technologiques ont également fait surgir de nouveaux risques importants et sont susceptibles d'avoir un effet délétère sur la dynamique des conflits. Plusieurs éléments suscitent des préoccupations.

Selon certaines estimations, le nombre d'incidents, commandités par des États ou non, impliquant une utilisation malveillante des technologies numériques à des fins politiques ou militaires a presque quadruplé depuis 2015. Les activités visant les infrastructures fournissant des services publics essentiels, tels que les organismes humanitaires et de santé, sont particulièrement inquiétantes. Dans le même temps, les armes létales autonomes poussent à s'interroger sur la responsabilité humaine en matière de recours à la force.

Comme l'a clairement indiqué le Secrétaire général, les machines qui ont le pouvoir et la capacité de tuer sans intervention humaine sont politiquement inacceptables, moralement répugnantes et devraient être interdites par le droit international. En outre, les acteurs non étatiques sont de plus en plus capables d'utiliser des technologies numériques peu onéreuses et largement disponibles pour atteindre leurs objectifs. Les groupes tels que Daech et Al-Qaida restent actifs sur les médias sociaux et utilisent des plateformes et des services de messagerie pour partager des informations et communiquer avec leurs partisans à des fins de recrutement, de planification et de collecte de fonds. La disponibilité croissante des méthodes de paiement numérique telles que les cryptomonnaies entraîne des difficultés supplémentaires.

D'autre part, les technologies numériques suscitent d'importantes préoccupations en matière de droits de l'homme, qu'il s'agisse des systèmes d'intelligence artificielle qui peuvent être discriminatoires ou de la disponibilité généralisée de technologies de surveillance qui peuvent être déployées pour cibler des communautés ou des personnes. Nous sommes également préoccupés par le recours croissant aux coupures d'Internet, notamment dans des situations de conflit actif, qui privent les populations de leurs moyens de communication et de leurs outils de travail et de participation politique.

Au Myanmar, par exemple, les coupures d'Internet et des services de téléphonie mobile se sont multipliées et prolongées depuis le coup d'État militaire du 1er février 2021, en particulier dans les zones où se déroulent des opérations militaires. Les médias sociaux peuvent alimenter la polarisation, et parfois la violence. L'utilisation abusive des médias sociaux et la réaction parfois limitée ou inadaptée des sociétés qui les dirigent favorisent la propagation de la désinformation, de la radicalisation, du racisme et de la misogynie. Cela peut accroître les tensions et dans certains cas exacerber les conflits. En Éthiopie, alors que les combats s'intensifiaient, le nombre de publications propageant des propos incendiaires sur les médias sociaux a connu une hausse alarmante, certaines allant jusqu'à inciter à la violence ethnique, comme l'a reconnu le Conseil de sécurité dans sa déclaration à la presse du 5 novembre 2021 (SC/14691).

Nous avons constaté que la désinformation et les discours de haine en ligne pouvaient causer des dommages hors ligne, notamment des violences. Nous savons que la désinformation peut entraver la capacité de nos missions de s'acquitter de leurs mandats en exacerbant les mensonges et en attisant la polarisation. Nous prenons toute une série de mesures pour atténuer ces risques dans le cadre de la Stratégie et du Plan d'action des Nations Unies pour la lutte contre les discours de haine, lancés par le Secrétaire général, et d'initiatives telles que Verified. En Iraq, par exemple, après la publication d'informations faisant état d'une aggravation du harcèlement en ligne ciblant les candidates à l'élection de l'année dernière, la Mission d'assistance des Nations Unies pour l'Iraq s'est associée à des organisations de la société civile pour surveiller les discours de haine, publier des rapports et sensibiliser davantage les électeurs.

Nous devons utiliser pleinement les possibilités qu'offrent les technologies numériques pour promouvoir la paix, mais ce faisant, nous devons également atténuer les risques que posent ces technologies et promouvoir leur utilisation responsable par tous les acteurs. Grâce à l'Assemblée générale, les États Membres ont considérablement progressé dans la création d'un cadre normatif visant à garantir un comportement responsable dans le cyberespace. Les États Membres contribuent également à l'élaboration et à la mise en œuvre d'une série de mesures de confiance visant à prévenir les conflits, à éviter les perceptions erronées et les malentendus et à réduire les tensions.

Il faut toutefois faire plus pour promouvoir, mettre au point et appliquer le cadre normatif émergent. Dans son rapport intitulé *Notre Programme commun* (A/75/982), le Secrétaire général a appelé à convenir d'un pacte numérique mondial, qui définirait les principes communs d'un avenir numérique ouvert, libre et sûr pour tout le monde. Si l'on ajoute d'autres aspects de *Notre Programme commun*, tels que le nouvel agenda pour la paix et la proposition d'adopter un code de conduite visant à promouvoir l'intégrité de l'information publique, une occasion cruciale se présente de bâtir un consensus

sur la manière dont les technologies numériques peuvent être utilisées pour le bien des personnes et de la planète, tout en s'attaquant aux risques qu'elles posent. L'action collective des États Membres reste cependant essentielle en vue d'atteindre cet objectif.

La Présidente (*parle en anglais*) : Je remercie M^me^ DiCarlo de son exposé.

Je donne maintenant la parole à M^me^ Nyabola.

M^me^ Nyabola (*parle en anglais*) : C'est un honneur et un plaisir pour moi de prendre la parole au Conseil de sécurité aujourd'hui sur la question des technologies numériques en rapport avec la paix et la sécurité. Comme les membres l'ont entendu à l'ouverture de la séance, je suis chercheuse et mes travaux portent sur les liens entre la technologie, la société et la politique. Je m'attache en particulier à approfondir notre compréhension collective des droits numériques.

Au cours des deux dernières décennies, nous avons été témoins d'une expansion considérable de l'utilisation des technologies numériques à tous les niveaux de notrevie sociale, que ce soit au niveau individuel, collectif, national ou transnational. Malheureusement, cette expansion n'a pas donné lieu à des efforts similaires pour nous protéger contre les dangers qu'elle a créés, ni à un engagement à comprendre et à défendre les droits de la personne humaine au sein du système que nous sommes en train de construire. Pour parler simplement, notre soif de numérisation dépasse notre connaissance de ses conséquences, et au regard des preuves de plus en plus nombreuses du tort que peut causer cette approche désordonnée, il est crucial de faire le point et de décider si nous devons modifier ou abandonner notre ligne de conduite.

Il serait insensé de tenter de résumer toutes les conséquences de l'ère numérique sur les droits dans le temps qui m'a été imparti. Je vais plutôt axer mon exposé sur certains problèmes d'ordre général créés par la numérisation et mentionner trois principes fondamentaux qui offrent des possibilités d'agir afin de préserver la paix et la sécurité.

En guise de préface, je souhaite nuancer mon propos en soulignant que le fait de parler des technologies numériques en rapport avec la paix et la sécurité ne doit pas être interprété comme une invitation à militariser ou à sécuriser Internet. Après tout, le Conseil est chargé de préserver la paix et la sécurité, et il est important de se laisser guider par un esprit qui est animé autant, sinon plus, par la volonté de réaliser une paix positive que par des considérations de sécurité. Internet est un espace d'innovation, de créativité et de possibilités formidables, et alors que nous réfléchissons à des moyens de régler les problèmes qui le touchent actuellement, j'exhorte le Conseil à s'engager à préserver Internet en tant que bien public mondial, de la même manière qu'un véritable esprit de coopération guide notre pensée sur des questions telles que l'Antarctique et l'espace extra-atmosphérique.

Néanmoins, après de longues années d'optimisme numérique débridé, nous sommes entrés dans une période de cynisme croissant, car les menaces qui ont été balayées d'un revers de la main alors que nous nous efforcions d'accélérer le progrès commencent à se manifester. Dans le cadre des recherches que je dirige avec Advox, nous utilisons une typologie simple pour comprendre ces menaces, en répartissant les domaines de la technologie numérique en quatre catégories : les données, l'accès, les discours et l'information.

Sur la question des pratiques concernant les données qui ciblent spécifiquement le stock de données, à l'instar de la surveillance ou de l'utilisation croissante de la biométrie, on constate une progression alarmante de l'économie de la surveillance mondiale, notamment l'utilisation généralisée de technologies telles que le logiciel Pegasus contre des dirigeants politiques, des journalistes et des membres de la société civile. Les technologies qui rendent ces pratiques possibles sont développées dans des pays riches puis déployées ou exportées dans des pays pauvres, sans aucune considération pour le contexte des droits de l'homme, exposant à un grave danger ceux qui sont en première ligne des initiatives de paix.

À cet égard, nous nous faisons l'écho du Haut-Commissariat des Nations Unies aux droits de l'homme en demandant instamment l'instauration d'un moratoire mondial sur la mise au point et la vente de technologies de surveillance, et nous invitons le Conseil de sécurité à contribuer à faire pression sur les sociétés privées afin qu'elles respectent ce moratoire. L'utilisation de technologies qui permettent aux entités étatiques et non étatiques de collecter des quantités massives de données, ou la « datafication » de nos vies, est également en hausse sans qu'il n'y ait d'effort correspondant pour protéger ou même faire connaître des droits fondamentaux tels que la confidentialité ou la protection des données. Dans les zones de conflit, la « datafication » de la vie des réfugiés a considérablement augmenté, notamment la collecte et le stockage de données biométriques sur les demandeurs

d'asile, qui sont conservées dans des conditions dénuées de toute transparence et qui sont parfois utilisées pour refuser des prestations aux réfugiés ou restreindre leurs libertés.

La question de l'accès porte sur des pratiques actives et passives qui limitent la capacité des personnes d'utiliser Internet, et qui vont des coupures d'Internet à la fermeture des médias sociaux en passant par les disparités de genre et le sous-investissement délibéré dans les infrastructures, au détriment des communautés à faible revenu. En 2021, l'organisation mondiale de défense des droits numériques Access Now a recensé 182 coupures d'Internet dans 34 pays, soit une augmentation par rapport aux 159 coupures enregistrées dans 29 pays en 2020. La plus longue coupure d'Internet a duré près de trois ans. Le pays le plus touché a connu 109 coupures d'Internet en un an.

En sus des coupures d'Internet, d'autres pratiques connexes se sont également accentuées, notamment la limitation de la bande passante et la fermeture des médias sociaux, en particulier durant les périodes de tensions électorales. Ces perturbations ont pour but de geler le discours et la participation civiques et sont un assaut direct contre la démocratie et la paix.

Plus généralement, il y a plusieurs pays où les femmes se heurtent toujours à des obstacles systématiques pour accéder à Internet, ce qui est devenu particulièrement visible quand les écoles du monde entier se sont essayées à l'enseignement virtuel face à la pandémie de maladie à coronavirus (COVID-19). Dans plusieurs pays où la transition ne s'est pas déroulée correctement, des jeunes filles ont été les plus touchées par l'exclusion de l'accès à la technologie disponible quelle qu'elle soit parce qu'elles étaient des filles. En outre, dans certains pays, y compris certains pays riches, bien qu'il y ait eu un progrès dans le fait de rendre la technologie numérique obligatoire pour la vie civique, notamment l'enregistrement des naissances, des décès et autres, l'investissement a été notablement faible dans le travail consistant à rendre les infrastructures numériques accessibles aux personnes en situation de handicap et ou dans les langues autochtones ou non majoritaires.

La question du discours concerne les restrictions aux libertés d'expression, d'information ou d'opinion. Dans de nombreux pays, les plateformes numériques fonctionnent de pair avec les plateformes analogiques, comme les médias et les places publiques, en tant qu'endroits où les gens peuvent se rassembler, délibérer et partager des idées sur la manière d'améliorer leur société. Il y a eu une augmentation marquée du recours à la législation pour limiter l'aptitude de la population à participer à de tels discours, notamment des lois qui élargissent injustement la définition de la diffamation criminelle pour frapper d'illégalité pratiquement toute critique des responsables publics. Le Haut-Commissariat des Nations Unies aux droits de l'homme a indiqué qu'au moins 40 lois sur les médias sociaux avaient été promulguées entre 2020 et 2021, et que 30 autres étaient à l'examen au cours de la même période.

Nombre de ces lois contiennent des définitions si larges des délits sous-jacents qu'elles sont censées réprimer qu'elles sont régulièrement utilisées avant tout contre les journalistes et les personnes qui critiquent l'État. La promulgation de ces lois est généralement suivie d'un pic du nombre de poursuites civiles et pénales contre des journalistes. Il convient de souligner ici qu'il y a souvent une dimension de genre à ces pratiques, sachant que des femmes journalistes comme Maria Ressa et Rana Ayyub, ou des membres de la société civile ou même de jeunes femmes ordinaires, sont spécifiquement prises pour cibles en raison de prétendues atteintes à la moralité publique ou simplement pour avoir fait leur travail.

Enfin, le domaine de l'information concerne des pratiques qui manipulent l'information dans la sphère publique afin de déformer la perception qu'ont les gens de la réalité et par conséquent perturber leur capacité d'agir comme il convient face aux problèmes sociaux et politiques. Il s'agit notamment de pratiques telles que la mésinformation, la désinformation et la malinformation, ainsi que le recours à des comportements inauthentiques coordonnés ou astroturfing pour biaiser l'opinion publique sur les plateformes de médias sociaux. Ces pratiques sont rendues possibles sur un Internet où la publicité est le moteur du trafic et où la perception de la popularité peut donc être achetée.

Dans les zones de conflit, les gouvernements hostiles ont recours à des comportements inauthentiques coordonnés pour faire taire les critiques en les bombardant de tant de commentaires négatifs que leurs médias sociaux deviennent inutilisables. Les administrations de plusieurs pays ont mis en place des services gouvernementaux spécialement conçus pour façonner le discours en ligne, ou des organismes ressemblant à des organes de presse pour déformer la perception de l'attitude de l'État ou polluer les lignes de communication avec tant de bruit que le signal ne peut

pas passer. Ces pratiques dans leur ensemble font qu'il est difficile de parvenir à la paix car elles font qu'il est difficile pour les gens de s'accorder sur les causes d'un conflit, et donc sur ce qui doit être fait pour l'arrêter.

Le principal motif d'inquiétude tient peut-être à ce que l'essor de ces pratiques ne se limite pas nécessairement à certains types de gouvernement ni à ceux que nous aurions tendance à qualifier d'autoritaires. Au lieu de cela, nos recherches font apparaître une tolérance croissante à ce que les préoccupations de sécurité nationale prennent le pas sur les préoccupations relatives aux droits humains et à la démocratie.

Je me dois de tirer la sonnette d'alarme au sujet de la pratique consistant à mettre au point et exporter des techniques permettant un autoritarisme numérique depuis des pays normalement démocratiques vers des pays explicitement autoritaires. Cela s'impose avant que nous ne nous occupions des injustices intégrées dans la technologie elle-même, notamment les inquiétudes quant aux injustices intégrées dans l'intelligence artificielle.

Dans le même temps, le fait de considérer les difficultés touchant Internet aujourd'hui comme des problèmes purement nationaux entraîne la fragmentation de la réponse réglementaire, et cela nuit à l'intérêt d'Internet comme connecteur. Nos recherches montrent que les menaces découlant de la numérisation sont multilatérales, c'est-à-dire qu'elles restent rarement confinées à un seul pays ; transnationales, car elles impliquent souvent le transfert de technologies par-delà les frontières nationales ; générationnelles, dans la mesure où nous hypothéquons la possibilité d'un Internet libre pour les générations futures sur la sécurité perçue du moment présent. Ces réalités appellent une réaction adaptée. Il ne suffit pas simplement de pointer tel ou tel pays du doigt. Nous devons identifier les cultures de l'autoritarisme numérique avant qu'elle ne s'enracinent et se propagent dans le monde.

Pour terminer, je tiens une fois de plus à rappeler le mandat du Conseil de sécurité qui consiste à préserver la paix et la sécurité et à encourager vivement une approche multilatérale, transnationale et générationnelle pour remédier aux problèmes relatifs aux droits humains dans l'ère numérique. Pour parvenir à une telle approche, j'exhorte le Conseil à garder à l'esprit trois principes.

Premièrement, les droits numériques sont des droits humains, et tout effort visant à régler ces problèmes doit commencer par la protection de l'humain des excès de pouvoir de l'État et des entreprises privées.

Deuxièmement, malgré ces problèmes et d'autres, la puissance d'Internet peut et doit être encore mise au service de l'intérêt commun, et nous devons façonner et protéger Internet comme un bien public mondial, sans laisser les considérations de sécurité ou le profit l'emporter sur les intérêts de la paix.

Troisièmement, quelque mesure que le Conseil choisisse de prendre doit porter au-delà du présent pour protéger les aspirations des générations futures. Quel avenir numérique partagé nos actions rendent-elles possible, et quels futurs circonscrivent-elles ? Évidemment, ces principes recèlent nombre de tensions et de contradictions. Voulons-nous plus de gouvernement, ou moins ? Quel rôle les entreprises privées devraient-elles jouer ? Comment trouvons-nous un équilibre entre notre volonté de progrès technique et notre souhait d'une utilisation holistique et équitable ?

Je pense qu'avec ces principes à l'esprit, on voit se dessiner certaines mesures que l'ONU peut prendre afin de protéger les droits numériques et de veiller à ce que les technologies numériques jouent un rôle positif dans la paix et la sécurité internationales. L'ONU doit continuer de se servir de son pouvoir rassembleur sans équivalent pour favoriser les débats et mobiliser un appui à la préservation d'Internet comme bien public mondial. L'ONU doit se servir de son pouvoir de définition de priorités pour faire en sorte que les droits humains soient intégrés rétroactivement et proactivement dans les technologies numériques que nous mettons au point et que nous utilisons. L'ONU doit se servir de son pouvoir de fixation de normes pour favoriser un accord sur les normes des droits de l'homme qui rendraient possible un avenir numérique libre, sûr et juste, non seulement pour la génération actuelle mais aussi pour celles qui suivront.

Enfin, l'ONU doit mobiliser un appui pour ceux qui jouent un rôle de premier plan dans ces efforts dans le monde entier, souvent aux prix de grands risques pour eux-mêmes, prenant la défense des personnes, comme Alaa Abd El-Fattah, qui subissent de graves injustices à cause de la manière dont elles utilisent Internet afin de promouvoir les idéaux démocratiques.

Aujourd'hui, nous sommes collectivement sur une trajectoire menant vers un avenir numérique injuste, mais une voie différente et plus juste est possible, et le Conseil a la possibilité de nous rapprocher de cet avenir meilleur.

La Présidente (*parle en anglais*) : Je remercie M^me^ Nyabola de son exposé.

Je donne maintenant la parole à M. Druet.

M. Druet (*parle en anglais*) : Je suis reconnaissant de cette occasion et de cet honneur de m'adresser au Conseil au sujet de la manière dont l'évolution des technologies numériques influe sur la nature des conflits violents et de l'effet que cela produit sur les efforts déployés par l'ONU pour prévenir la violence, pérenniser la paix et atténuer la souffrance et la guerre.

Comme la Présidente du Conseil l'a indiqué, j'ai participé au développement des capacités technologies de l'ONU pendant plusieurs années, notamment en ce qui concerne la perception de la situation, l'analyse et le renseignement au service du maintien de la paix. À présent, je conduis des recherches sur ces questions à l'Université McGill et conseille diverses parties prenantes sur les croisements entre la technologie, la nature des conflits et les interventions en faveur de la paix et de la sécurité internationales.

Aujourd'hui, je souhaite donner mon point de vue sur trois thèmes liés entre eux : premièrement, la façon dont les technologies numériques sont en train de reconfigurer les conflits dont le Conseil de sécurité est saisi ; deuxièmement, la façon dont ces technologies et leur utilisation par les parties aux conflits et l'ONU elle-même influe sur les efforts déployés par l'Organisation afin de prévenir et d'éliminer la violence ; troisièmement, la façon dont la boîte à outils de l'ONU pour la paix et la sécurité, en particulier les opérations de paix, peut être adaptée pour fonctionner de manière plus efficace et responsable dans ces contextes évolutifs.

S'agissant du premier thème, sur l'incidence, le Conseil a déjà entendu à maintes occasions comment les technologies numériques ont servi d'accélérateurs des dynamiques au sein et à l'extérieur des groupes, de plateformes pour la propagation rapide des contre-discours et de la mésinformation, et d'outils de manipulation des populations, notamment par les États, les acteurs non étatiques et les extrémistes. Au Myanmar, par exemple, il est bien établi que l'incitation anarchique à la violence sur Facebook et les algorithmes qui ont mis en évidence des idées extrêmes ont contribué à la violence génocidaire contre le peuple rohingya. Depuis lors, l'accès à Internet et aux moyens de communication est utilisé pour contrôler les populations réfugiées à Cox's Bazar. Plus récemment, le conflit en Ukraine a mis en évidence le rôle central de la rhétorique publique dans les stratégies de la plupart des parties à un conflit moderne, sinon toutes.

Dans bon nombre de conflits et de contextes précaires pour lesquels l'ONU est mobilisée, il importe de relever que les populations sont clairement vulnérables à la désinformation et à la mésinformation. Certains pays, tels que la République centrafricaine, n'ont pas une culture journalistique professionnelle ou une infrastructure des médias au sens traditionnel, donc la population dépend presque exclusivement des médias sociaux pour s'informer. En outre, alors que les entreprises de médias sociaux parlent beaucoup de leurs activités pour lutter contre la désinformation sur leurs plateformes, la divulgation de documents internes à Facebook en 2021 a révélé que les ressources consacrées à la modération de contenus concernaient essentiellement les États-Unis et l'Occident, tandis que certains milieux fragiles et situations de conflit étaient pratiquement ignorés. À cet égard, le Conseil de sécurité a l'occasion d'exiger des entreprises de médias sociaux qu'elles s'acquittent de leurs obligations de la même manière dans toutes les régions du monde où elles sont présentes.

Outre leur incidence sur la dynamique des conflits, les technologies numériques jouent un rôle de plus en plus important en matière de protection ou de privation des droits humains en situation de conflit. En Afghanistan, des civils ont mentionné les répercussions du bourdonnement omniprésent des drones sur leur santé mentale, tandis qu'au Myanmar, la junte militaire a utilisé le contrôle qu'elle exerce sur Internet pour cibler les opposants au coup d'État de 2021 et limiter leur capacité à communiquer et à s'organiser. Pendant la crise des migrants provoquée par le conflit en Syrie et, plus récemment, le conflit en Ukraine, des questions importantes se sont fait jour concernant le consentement éclairé pour la collecte et la gestion des données biométriques, y compris par les acteurs humanitaires.

S'agissant du deuxième sujet, à savoir l'incidence des technologies numériques sur les opérations de paix, au fur et à mesure que les technologies numériques et la rhétorique utilisée gagnent en importance pour la logique de guerre, les opérations des Nations Unies déployées dans ces situations de conflit ont été inévitablement incorporées aux stratégies des parties au conflit pour influencer le résultat en leur faveur. Ainsi, la Mission multidimensionnelle intégrée des Nations Unies pour la stabilisation en République centrafricaine a été la cible de campagnes visant délibérément à saper sa crédibilité auprès de la population. Les motivations de ces activités semblent très différentes selon le contexte et les acteurs concernés. Par exemple, la

désinformation ciblant la Mission multidimensionnelle intégrée des Nations Unies pour la stabilisation au Mali menée par certains potentats locaux semble avoir pour but de compromettre les opérations de la Mission qui perturberaient les filières économiques illégales. Dans d'autres situations, les acteurs de la désinformation paraissent motivés par des objectifs idéologiques, tandis que dans d'autres situations encore, l'ONU semble servir de bouc émissaire à un État hôte ou à ses partenaires qui cherchent à détourner l'attention de leurs performances en matière de sécurité et de services à la population. Quelles que soient leurs motivations, ces attaques réduisent sérieusement l'accès de l'ONU aux populations locales dans le besoin, nuisent à ses relations avec les gouvernements hôtes et les parties aux processus de médiation et de paix et, dans certains cas, mettent vraiment en péril la sûreté et la sécurité des soldats de la paix.

Cependant, il est tout aussi important de reconnaître le rôle joué par les technologies numériques pour permettre à l'ONU d'exécuter efficacement ses mandats dans les contextes de conflit moderne. Les opérations de paix des Nations Unies en Somalie et au Mali, par exemple, font appel aux technologies de traitement du langage naturel pour pouvoir rapidement comprendre les nuances des perceptions locales et du discours politique national. Des technologies de contrôle et de surveillance telles que les systèmes de drones non armés sont intégrées de plus en plus efficacement aux outils de collecte de données qualitatives et quantitatives et aux systèmes d'analyse à l'échelle des missions pour obtenir des renseignements de meilleure qualité en vue du maintien de la paix. Cela permet de mieux détecter les menaces et d'agir plus rapidement pour protéger les civils et, bien sûr, garantir la sûreté et la sécurité du personnel des Nations Unies.

Dans ce contexte, j'aimerais soumettre à l'examen du Conseil quelques pistes de réflexion sur la manière dont l'ONU peut s'adapter aux effets des technologies numériques sur les conflits, réduire les conséquences négatives de ces technologies sur ses opérations et les utiliser de manière plus efficace et responsable dans ces contextes. À cet égard, je vois quatre priorités principales.

Premièrement, l'ONU doit assumer un rôle plus évident et énergique en tant qu'acteur de l'information dans les contextes de conflit. L'accès à des informations exactes peut être de plus en plus considéré comme un droit fondamental dans les situations de guerre de l'information, et l'ONU doit jouer un rôle pour faire connaître la vérité et diffuser des informations fiables. Je dois souligner que c'est un rôle que les missions des Nations Unies jouent depuis plusieurs années dans le cadre des mécanismes des processus de paix, par exemple, le suivi des cessez-le-feu. Par conséquent, il convient d'examiner de quelle manière on pourrait tirer parti des bonnes pratiques développées grâce à ces mécanismes pour mieux informer les populations en situation de conflit.

Toutefois, pour que l'ONU puisse jouer un tel rôle, il est impératif que ses opérations gagnent et conservent la confiance des différents groupes de population. Ce n'est pas une tâche aisée, puisque certaines activités des Nations Unies, comme la protection des civils ou l'appui apporté aux autorités de l'État hôte, peuvent exposer les missions à des critiques, qui sont parfois justifiées, parfois non, et le risque est encore plus grand lorsqu'elles sont la cible de campagnes de désinformation. C'est pourquoi la deuxième priorité consiste à renforcer considérablement les capacités des opérations de paix des Nations Unies de surveiller et analyser l'espace de l'information et de réagir efficacement face aux communications malveillantes. Selon un rapport récent de l'International Peace Institute, les missions doivent anticiper les crises et recentrer la communication en amont, procéder à un dialogue et non à une communication à sens unique et adapter leurs messages à des publics spécifiques.

Troisièmement, l'ONU devra se doter de nouvelles technologies et des capacités nécessaires pour les utiliser efficacement, tant dans le domaine des communications que dans ceux de l'appréciation des situations et du renseignement aux fins du maintien de la paix, de l'analyse des données en vue d'une planification stratégique, et des nouvelles technologies au service du dialogue et de la médiation, pour ne donner que quelques exemples. À mesure que l'ONU continue d'adopter de nombreuses innovations prometteuses dans ces domaines, y compris celles soulignées par M^me^ DiCarlo, il est essentiel de reconnaître que ces outils posent des questions éthiques, juridiques et politiques importantes et complexes qui ont une incidence sur les droits des personnes qui souffrent déjà à cause des conflits. Bien qu'il puisse être tentant d'adopter les cadres et la doctrine des États Membres concernant l'utilisation de ces outils, j'arguerais ici que les opérations des Nations Unies répondent à des intérêts et des responsabilités distincts lorsqu'elles utilisent des technologies sensibles dans des situations de conflit.

C’est pourquoi en quatrième lieu, je voudrais insister sur l’importance, pour la crédibilité et le positionnement politique des missions sur le terrain, des modalités d’acquisition et d’utilisation de nouvelles technologies par l’ONU. L’expérience a montré que l’acquisition de nouvelles technologies sensibles et la mise en place de partenariats en la matière sont plus efficaces lorsqu’elles renforcent l’impartialité de l’ONU et fournissent des garanties crédibles au public qu’elles seront utilisées de manière responsable.

Par conséquent, j’exhorte le Secrétariat à développer des outils, politiques et procédures qui lui sont propres et qui tiennent compte du caractère spécifique de l’ONU en tant qu’utilisatrice de ces technologies. Des travaux importants sont déjà en cours à cet effet, notamment au sein du Département des opérations de paix, qui s’emploie à étoffer ses politiques de contrôle et de suivi, ainsi que dans le cadre des efforts déployés à l’échelle des Nations Unies, sous l’impulsion de l’initiative Global Pulse de l’ONU, pour mettre en place une politique de confidentialité des données dans l’ensemble du système. Si ces efforts sont déployés correctement et en toute transparence pour les États Membres et le public, je pense qu’ils permettront d’instaurer des normes quant à l’utilisation responsable des technologies sensibles dans les situations de conflit où des populations vulnérables sont concernées.

Ces efforts doivent s’accompagner d’une réflexion franche sur les limites de la capacité de l’ONU de protéger les informations sensibles, en particulier les renseignements personnels, contre les intrusions d’acteurs étatiques et non étatiques, ainsi que d’un examen ultérieur des pratiques concernant, par exemple, la collecte de données biométriques effectuée dans le cadre des opérations humanitaires. Cet examen devrait également inclure l’élaboration de directives supplémentaires sur la manière dont l’ONU partage les informations avec des forces non onusiennes, y compris les forces militaires parallèles, les autorités du pays hôte et les acteurs internationaux de l’état de droit, conformément à la politique de diligence voulue en matière des droits humains de l’ONU.

Pour conclure, le débat d’aujourd’hui porte sur deux séries de questions très distinctes, mais intimement liées : premièrement, la manière dont les technologies numériques modifient la nature des conflits dans les situations où les Nations Unies sont engagées ; et, deuxièmement, la manière dont l’ONU elle-même utilise les technologies numériques au service de ses mandats. Toutes deux requièrent un examen et un débat nuancés, ainsi que des réponses politiques et opérationnelles différentes. Pour que nos opérations actuelles et futures soient couronnées de succès, nous devons bien appréhender ces deux séries de questions. Le Conseil de sécurité a un rôle crucial à jouer à cet égard.

La Présidente (*parle en anglais*) : Je remercie M. Druet de son exposé.

J’appelle l’attention des orateurs et oratrices sur le paragraphe 22 de la note du Président publiée sous la cote S/2017/507, qui encourage tous les participants aux séances du Conseil de sécurité à faire leurs déclarations en cinq minutes ou moins, conformément à l’engagement du Conseil de sécurité de faire un meilleur usage des séances publiques.

Je vais maintenant faire une déclaration en ma qualité de représentante des États-Unis.

Je remercie la Secrétaire générale adjointe DiCarlo de son exposé. Ses observations indiquent clairement que les nouvelles technologies jouent déjà un rôle clef dans les efforts de maintien de la paix de l’ONU et qu’il est essentiel qu’elles soient utilisées de manière constructive. Je remercie M^me^ Nyabola d’avoir partagé son point de vue extrêmement précieux sur les avantages que les militants des droits de l’homme et la société civile peuvent tirer de l’utilisation potentielle de ces technologies, mais aussi sur les défis auxquels ils se heurtent, y compris du fait de leur utilisation abusive. Je remercie M. Druet d’avoir mis en lumière les façons dont la technologie numérique peut être utilisée pour appuyer le travail des soldats de la paix, et dont son utilisation abusive peut le compromettre. Je voudrais optimiser la première et réduire au minimum la seconde. La présente séance d’information porte sur une occasion énorme et un défi pressant.

Le Conseil de sécurité a en effet l’occasion d’exploiter le pouvoir de la technologie numérique pour promouvoir la paix et la sécurité grâce à une utilisation responsable de ces outils afin d’apporter d’énormes bienfaits dans les conflits et les contextes mêmes où ils font du tort. Après tout, ces technologies recèlent un immense potentiel pour contribuer à l’œuvre accomplie par le système des Nations Unies à travers le monde. Les outils des médias sociaux et les applications de messagerie peuvent faciliter l’accès à des informations vitales avant et pendant un conflit. Les données fournies par les satellites permettent d’identifier les risques liés aux changements climatiques, de fournir

des informations essentielles aux soldats de la paix et d'améliorer les communications d'urgence pendant les conflits et les catastrophes naturelles. Nous pouvons identifier et arrêter les famines avant qu'elles ne commencent. Nous pouvons trouver des logements et des emplois pour les réfugiés. Nous pouvons mieux protéger les soldats de la paix et les personnes qu'ils ont pour mission de servir.

Mais nous devons également relever un défi urgent, à savoir l'utilisation abusive des technologies numériques pour restreindre les droits de l'homme et alimenter les conflits. Entre les mains d'acteurs étatiques et, dans certains cas, d'acteurs non étatiques, ces technologies sont utilisées pour couper l'accès à l'information, réprimer la liberté d'expression et propager de fausses informations, ce qui a pour effet d'intensifier les conflits et de saper les valeurs fondamentales énoncées dans la Charte des Nations Unies que nous sommes chargés de défendre.

En République centrafricaine et au Mali, la désinformation ciblant les missions de maintien de la paix des Nations Unies a menacé la sûreté et la sécurité des soldats de la paix et sapé la capacité des missions de protéger les civils. En Éthiopie, les autorités ont coupé l'accès à Internet dans la région du Tigré depuis novembre 2020, en raison du conflit qui a éclaté entre les Forces éthiopiennes de défense nationale et les forces régionales du Tigré. Ces actions entravent la capacité des civils d'accéder aux services de santé, retardent la collecte d'informations sur les atrocités et les atteintes aux droits de l'homme, perturbent les services financiers et empêchent les familles de se connecter virtuellement à leurs proches.

Certains pays assis à cette table utilisent également la technologie pour harceler, surveiller arbitrairement, censurer et réprimer la société civile et les médias indépendants comme jamais auparavant. Cela est particulièrement évident dans le cadre de la guerre que la Russie a choisi de mener contre l'Ukraine. Le Gouvernement russe continue de fermer, de restreindre et de dégrader la connectivité Internet, de censurer des contenus, de propager de fausses informations en ligne et d'intimider et d'arrêter les journalistes qui diffusent la vérité sur son invasion. Ces pratiques sont aussi dommageables qu'elles sont répandues. Comme l'a dit M^me^ Nyabola, l'organisation non gouvernementale Access Now estime qu'en 2021, il y a eu 182 coupures d'Internet dans 34 pays. Plus troublant encore, on entend souvent dire que ces mesures sont prises au nom de la protection de la paix et de la sécurité. Rien n'est moins vrai.

Nous continuons également de voir des acteurs non étatiques, notamment des terroristes et des extrémistes violents, utiliser des plateformes de communication en ligne pour recruter, radicaliser et mobiliser en faveur de la violence. Tous ceux qui, parmi nous, ont la volonté de combattre et de prévenir les conflits dans le monde doivent jouer leur rôle pour que les technologies soient une force de changement positif, et non un outil utilisé à mauvais escient pour perpétrer des atteintes aux droits de l'homme, alimenter la haine et exacerber les conflits.

C'est pourquoi les États-Unis collaborent avec la société civile, le secteur privé et d'autres parties prenantes pour promouvoir cet effort mondial. Pour notre part, nous dénonçons le recours aux fermetures partielles et complètes de l'accès à Internet, à la censure et à d'autres tactiques visant à empêcher l'exercice de la liberté d'expression en ligne. Dans le prolongement du Sommet pour la démocratie, nous continuons d'unir nos forces à celles de nos partenaires de la Coalition pour la liberté en ligne afin de protéger la liberté sur Internet et de veiller à ce que l'ensemble des écosystèmes numériques respectent les cadres internationaux en matière de droits de l'homme.

Nous savons que les outils de surveillance et autres technologies à double usage peuvent être utilisés à mauvais escient pour menacer les défenseurs des droits de l'homme et d'autres personnes. C'est pourquoi nous utilisons les contrôles à l'exportation pour placer devant leurs responsabilités les entreprises qui développent, commercialisent ou utilisent des logiciels espions et d'autres technologies qui permettent de telles activités malveillantes.

Nous travaillons dans le cadre de l'ONU et d'autres instances pour défendre le cadre de comportement responsable des États dans le cyberespace, qui précise que le droit international s'applique aux cyberactivités des États et établit un ensemble de normes volontaires pour guider leur comportement en temps de paix. Nous faisons également front commun avec des pays du monde entier pour nous protéger contre les cyberactivités malveillantes et y répondre. À travers le monde, des formes de harcèlement et d'abus en ligne liées au genre, y compris des campagnes de désinformation contre des dirigeantes, perturbent la participation des femmes sur un pied d'égalité à la prise de décision sur les questions de paix et de sécurité.

Nous devons œuvrer de concert pour combattre la mésinformation et la désinformation au niveau mondial. L'ONU joue déjà un rôle clef en produisant des informations transparentes et facilement accessibles et en défendant les intérêts des journalistes en première ligne.

Nous devons également saisir les occasions d'exploiter le potentiel latent des technologies pour promouvoir la paix et la sécurité. Le mois dernier, un groupe de 60 partenaires mondiaux a ainsi lancé une Déclaration sur l'avenir de l'Internet afin d'insuffler un nouvel élan à la vision démocratique de l'Internet mondial. Nous invitons toutes les autorités compétentes et les États Membres de l'ONU qui sont attachés aux principes énoncés dans la Déclaration à se joindre à nous.

Pour maintenir efficacement la paix et la sécurité au XXIe siècle, nous devons répondre aux menaces du XXIe siècle et déployer des outils du XXIe siècle. L'heure est venue pour l'ONU d'exploiter de manière responsable le pouvoir de la technologie numérique pour relever les défis les plus pressants et promouvoir la paix et la sécurité dans le monde.

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

M. Hoxha (Albanie) (*parle en anglais*) : Nous remercions les États-Unis d'avoir organisé cette séance opportune pour parler d'un sujet aussi complexe qu'important. Nous remercions également la Secrétaire générale adjointe DiCarlo de ses perspectives toujours aussi éclairées.

Nous nous félicitons de la place de choix accordée aux représentants de la société civile à la présente séance, qui est totalement justifiée, comme en témoignent l'ampleur de leurs contributions et les recommandations qu'ils ont formulées. Aussi voudrais-je remercier Mme Nyabola et M. Druet.

Le développement rapide de la technologie a changé la façon dont le monde fonctionne, influant sur chaque aspect de la vie moderne. Elle est tellement ancrée dans notre vie quotidienne qu'il est difficile de se souvenir de ce qu'était le monde avant.

La technologie moderne apporte indéniablement de nombreux avantages dans de multiples secteurs. Les personnes, les États, les gouvernements, l'industrie, les soins de santé, les systèmes financiers, les organisations régionales et internationales et les missions de maintien de la paix profitent tous de l'essor rapide des technologies numériques. Ces technologies aident les personnes à être plus productives et les entreprises et les organisations à être plus innovantes, plus souples et plus adaptables que jamais.

Nous avons accueilli à bras ouverts les appareils et les systèmes interconnectés, qui ont considérablement simplifié notre vie et notre travail, mais cette évolution nous expose inévitablement à toute une série de menaces émanant de forces malveillantes. Nul besoin d'expliquer le lien entre les nouvelles technologies et les nouvelles menaces.

Comme nous l'avons entendu aujourd'hui, tout le monde a conscience des risques énormes découlant des activités malveillantes d'acteurs étatiques et non étatiques. L'utilisation à mauvais escient des technologies de l'information et des communications a des conséquences directes sur la paix et la sécurité internationales, car elle porte atteinte à l'intégrité, à la sécurité, à la croissance économique et à la stabilité de la communauté internationale, provoquant des différends et des conflits.

Compte tenu des préoccupations croissantes concernant les technologies à double usage et leurs incidences sur le maintien de la paix et de la sécurité internationales, il est primordial que le Conseil de sécurité joue un rôle de premier plan dans l'évaluation de ces risques et répercussions. Je me félicite donc vivement de la tenue de la séance d'aujourd'hui.

L'intelligence artificielle fait des merveilles dans de nombreux secteurs, notamment l'agriculture et la médecine : elle permet de sauver des vies, d'accroître la production alimentaire, d'améliorer les sources d'énergie et de gérer les processus de production. Toutefois, si elle n'est pas utilisée correctement et, surtout, si elle ne respecte pas les normes éthiques, elle peut entraîner de graves violations des droits humains, comme la surveillance excessive de certains groupes et de certaines communautés. Comme les technologies évoluent généralement à un rythme trop rapide pour que les États puissent appréhender tous leurs effets, nous devons veiller à ce que les principes et valeurs fondamentaux, tels que l'équité, l'égalité, l'inclusion, la responsabilité, la transparence et l'obligation de rendre des comptes, soient préservés de tout effet néfaste.

Malheureusement, la technologie peut avoir des répercussions dramatiques sur la cohésion sociale et, bien sûr, sur la paix et la sécurité internationales, si elle est utilisée à mauvais escient par des acteurs étatiques

ou non étatiques. Certains pays essaient sans cesse de diffuser délibérément des informations trompeuses, de déformer la réalité, de s'immiscer dans les processus démocratiques d'autres pays, de répandre la haine, de promouvoir la discrimination et d'inciter à la violence ou aux conflits en utilisant de manière abusive les technologies numériques. Dans le même ordre d'idées, nous constatons avec inquiétude des fermetures d'Internet, ainsi que la limitation ou le déni des droits humains et des libertés. Les intervenants ont donné des exemples concrets. Nous devons redoubler d'efforts pour atténuer les préjudices que les technologies risquent d'occasionner, comme le souligne le rapport du Secrétaire général sur un plan d'action de coopération numérique (A/74/821), et examiner attentivement ses recommandations.

Je tiens à souligner la position ferme de l'Albanie en faveur d'un cyberespace mondial, ouvert, libre, stable et sûr, où le droit international, y compris le respect des droits humains et des libertés fondamentales, s'applique pleinement, à l'appui du développement socioéconomique et politique.

Nous sommes très préoccupés par la multiplication des activités cybernétiques et numériques malveillantes au cours des derniers mois. Nous savons que les actions de la Russie ont entraîné une interruption des communications, touchant notamment des infrastructures critiques, non seulement en Ukraine mais aussi dans d'autres pays d'Europe, suite à une attaque délibérée contre le satellite Viasat le 24 février dernier, une heure seulement avant l'invasion non provoquée et injustifiée de l'Ukraine par la Russie.

Des cyberattaques auraient également été lancées à partir de la Russie pour tenter d'interférer dans les élections ukrainiennes, en ciblant le réseau électrique du pays, en défigurant les sites Web gouvernementaux et en propageant des logiciels malveillants dans les systèmes, avec des conséquences dévastatrices. Les Balkans occidentaux, dont je suis originaire, sont systématiquement visés par des campagnes d'ingérence et de manipulation de l'information afin de déclencher intentionnellement une instabilité politique et de saper leurs aspirations euro-atlantiques. Nous ne tolérerons pas ces actes, et nous nous y opposerons.

Un autre exemple notoire qu'on peut citer, ce sont les activités malveillantes répétées du régime de la République populaire démocratique de Corée, qui essaie de recueillir des renseignements, de lancer des cyberattaques et de générer des revenus illicites, qui sont notamment utilisés pour financer les efforts de militarisation du pays et son programme de prolifération nucléaire, en violation du droit international et des résolutions du Conseil de sécurité. Nous pouvons ajouter à cette liste la coupure d'Internet au Myanmar, qui a également été mentionnée aujourd'hui. Nous appelons à la cessation de ces activités et au respect des normes existantes et de l'ordre international fondé sur des règles dans le cyberespace. Internet n'est pas, et ne doit pas devenir, une arme, mais rester un bien public.

Nous nous félicitons des rapports présentés par le Groupe d'experts gouvernementaux et le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Grâce à eux, les États Membres se sont mis d'accord sur un cadre solide des Nations Unies qui comprend le droit international en vigueur, 11 normes d'application volontaire non contraignantes, des mesures de confiance et de renforcement des capacités et l'expertise des différentes parties prenantes.

Pour conclure, je tiens à dire que, tout au long de l'histoire, les nouveaux défis ont donné lieu à de nouvelles possibilités de coopération. Il en va de même aujourd'hui, même si les défis à relever sont extrêmement complexes, évoluent rapidement et s'inscrivent dans un contexte d'exacerbation des conflits et des crises. Il n'y a cependant pas d'autre option qu'un dialogue constructif, la coopération sur la base de comportements responsables et des cadres normatifs relatifs aux incidences des progrès technologiques sur les personnes, les États et les sociétés et aux utilisations et applications de la technologie qui engendrent le plus de perturbations, notamment celles qui constituent une menace directe pour la paix et la sécurité. Comme dans de nombreux autres domaines, c'est à nous de décider si nous voulons partager les immenses avantages ou supporter les énormes coûts.

M. de Rivière (France) : Je remercie M^me^ DiCarlo, M^me^ Nyabola et M. Druet pour leurs présentations.

Je mettrai l'accent sur trois points.

Premièrement, les technologies numériques sont une opportunité pour la paix et la sécurité internationales. Les opérations de maintien de la paix ont été à la pointe de ces efforts. La déclaration présidentielle adoptée en août dernier (S/PRST/2021/17) à l'initiative de l'Inde en a dressé le bilan. Ces technologies contribuent à la sécurité des Casques bleus et à la performance des

opérations, notamment pour améliorer la protection des civils. Elles révolutionnent la communication stratégique du maintien de la paix. La France continuera donc de soutenir l'ensemble de ces innovations.

Les technologies sont aussi un levier pour mobiliser et inclure la société civile. Au Soudan, la Mission intégrée des Nations Unies pour l'assistance à la transition au Soudan a réalisé une consultation en ligne qui a permis à l'ensemble de la société civile de faire entendre sa voix, y compris dans les régions. En facilitant la circulation de l'information, les technologies contribuent aussi à la lutte contre l'impunité, comme l'illustrent la couverture médiatique et le renseignement en source ouverte dans le contexte du conflit en Ukraine.

Deuxièmement, les usages malveillants des technologies prolifèrent et peuvent aussi constituer une menace pour la paix et la sécurité internationales.

Je pense tout d'abord au développement de la cybermenace, comme l'illustre là encore le conflit en Ukraine. La France et l'Union européenne, ainsi que plusieurs partenaires, ont notamment condamné la cyberattaque conduite par la Russie contre un réseau de satellites une heure avant l'invasion de l'Ukraine dans l'objectif de faciliter son agression. Le droit international s'applique dans son intégralité au cyberspace. Nous condamnons aussi les cyberactivités malveillantes de la Corée du Nord consistant à voler des informations sensibles et des cryptomonnaies pour contribuer aux programmes nucléaire et balistique. Nous sommes aussi préoccupés par l'usage croissant des cryptomonnaies pour le financement du terrorisme. Nous condamnons l'intensification des attaques contre les acteurs humanitaires et les organisations non gouvernementales.

Les technologies numériques facilitent aussi la guerre de l'information. Nous condamnons les campagnes de désinformation massive en cours en République centrafricaine et au Mali, ainsi que celles qui accompagnent la guerre menée par la Russie contre l'Ukraine. Au Mali, la France a récemment déjoué une grossière tentative de manipulation de l'information par les mercenaires du groupe Wagner. Cet exemple montre la menace que représentent les stratégies hybrides qui cherchent à brouiller la frontière entre acteurs étatiques et non étatiques.

La coupure d'Internet porte atteinte aux droits de l'homme. Nous déplorons l'interruption des télécommunications toujours en cours dans le nord de l'Éthiopie. Elle a compliqué le recueil des preuves des violations des droits de l'homme, qui ne doivent pas rester impunies. Au Moyen-Orient, la coupure d'Internet est utilisée pour affaiblir les mouvements de contestation, et certains défenseurs des droits sont surveillés et harcelés sur les réseaux sociaux.

Troisièmement, face à la multiplication de ces menaces, les gouvernements doivent répondre par la coopération et le droit.

Les Nations Unies offrent un cadre irremplaçable pour y parvenir. La France continuera d'y contribuer, y compris en veillant à ce que les résolutions du Conseil de sécurité tiennent compte de ces défis. Avec un groupe de 60 pays, nous promouvons l'établissement au sein de l'ONU d'un programme d'action visant à augmenter la capacité des États de mettre en œuvre les normes agréées dans le cyberespace et à renforcer la résilience des réseaux.

M. Tirumurti (Inde) (*parle en anglais*) : Je me félicite de l'initiative prise par les États-Unis d'organiser l'importante séance d'aujourd'hui. Je remercie de leurs précieuses observations la Secrétaire générale adjointe aux affaires politiques et à la consolidation de la paix, M^me^ Rosemary DiCarlo, et les autres intervenants, M^me^ Nyabola et M. Druet.

L'utilisation croissante des technologies numériques a accéléré le développement économique, amélioré la prestation de services aux citoyens, généré une conscience sociale plus poussée et placé l'information et la connaissance directement entre les mains des individus. Ces technologies ont rendu la gouvernance plus inclusive, plus centrée sur le citoyen et plus transparente. À l'ère numérique, la plupart des activités, qu'elles soient sociopolitiques, économiques, humanitaires ou de développement, sont désormais invariablement menées dans le cyberespace ou liées à celui-ci. Cependant, étant donné leur nature à double usage et leur vulnérabilité aux utilisations malveillantes par des acteurs étatiques comme non étatiques, elles peuvent également avoir des conséquences néfastes sur la paix et la sécurité internationales.

La nature des conflits et les éléments qui les sous-tendent ont considérablement évolué au fil des décennies. Alors que les conflits interétatiques se poursuivent, nous sommes témoins de menaces croissantes émanant d'acteurs non étatiques, notamment de groupes terroristes. De même, les théâtres de guerre et de conflit se sont étendus. Outre les conflits territoriaux, le monde est confronté à des conflits plus

récents dans les mers et dans l'espace, et par espace, j'entends à la fois l'espace extra-atmosphérique et le cyberespace. Dans ces conflits, la technologie est devenue le dénominateur commun sous-jacent, ainsi qu'un élément qui change la donne. Par conséquent, notre approche conventionnelle de la sécurité nationale et internationale doit être repensée.

Je voudrais soumettre les cinq questions suivantes au Conseil de sécurité pour examen. Premièrement, il convient de prendre des mesures pour faire face à l'utilisation abusive des technologies numériques par les groupes terroristes pour diffuser des idéologies terroristes, radicaliser, inciter à la violence et recruter la prochaine génération d'acteurs terroristes en tirant parti de la présence d'un plus grand nombre de jeunes en ligne. Les groupes terroristes mettent à profit les outils en ligne pour créer des réseaux, recruter de nouveaux membres, se procurer des armes et mobiliser un appui logistique. Les moyens de communication numérique utilisés par ces groupes sont organisés et sophistiqués. Ils sont passés maîtres dans l'art d'utiliser les salons de discussion sur les jeux, le dark Web et d'autres sites d'accès restreint, ainsi que les espaces en ligne non réglementés, pour diffuser leur propagande et inciter à la violence. Il est arrivé que des terroristes diffusent leurs attaques en direct sur les principales plateformes afin d'en maximiser le retentissement. La capacité de l'espace en ligne de toucher un vaste public a permis aux groupes terroristes de tirer parti de l'ouverture des sociétés démocratiques pluralistes, comme la nôtre, en alimentant les divisions sociétales et la haine sectaire et en appuyant les mouvements antidémocratiques et les idéologies radicales visant à déstabiliser les gouvernements et les institutions publiques.

La capacité des acteurs terroristes de se connecter, de communiquer et de partager des informations sur des plateformes numériques ne fait que souligner la nécessité croissante de réglementer ces contenus incendiaires en ligne. Il convient tout autant de s'attaquer aux problèmes juridiques qui se posent pour ce qui est de traduire les auteurs de ces crimes en justice, en particulier en raison du fait qu'ils mènent leurs activités terroristes à distance. Alors que nous avons l'habitude de considérer le terrorisme comme une attaque physique directe perpétrée par les auteurs, dans le domaine numérique, les personnes qui incitent à des actes terroristes en diffusant des contenus haineux et des idéologies radicales peuvent être éloignées des personnes qui commettent effectivement l'acte terroriste. Les personnes qui fomentent des actes terroristes doivent être tenues pour responsables de ces actes dans la même mesure que celles qui les commettent. Elles ne peuvent être moins coupables. Cet aspect est essentiel quand nous parlons du terrorisme dans le cyberespace.

L'émergence de nouvelles technologies financières telles que les nouvelles méthodes de paiement, les monnaies virtuelles et les méthodes de collecte de fonds en ligne, notamment les dons directs, les jetons non fongibles et les plateformes de financement participatif, ainsi que leur facilité d'accès, leur anonymat et leur non-traçabilité, permettent aux entités terroristes de collecter et de transférer des fonds tout en échappant aux structures de surveillance et de répression. Les nouvelles méthodes de paiement telles que les cartes téléphoniques prépayées, les services de paiement en ligne et la monnaie virtuelle permettent aux groupes terroristes de les échanger contre de l'or, de l'argent et d'autres métaux et, plus récemment, contre des paiements par téléphone mobile, et de financer des activités terroristes. Les cartes prépayées sont fréquemment utilisées comme solution de substitution à l'argent liquide. Il est également bien connu que les bitcoins sont utilisés pour financer des activités terroristes. En outre, l'utilisation abusive par les terroristes de l'intelligence artificielle et de l'impression 3D à diverses fins terroristes, qui ont une portée mondiale, requiert également notre attention immédiate.

La nécessité pour les États Membres d'aborder et de traiter de manière globale et plus stratégique les conséquences de l'exploitation des technologies numériques à des fins terroristes n'a jamais été aussi pressante. À cet égard, j'ai le plaisir d'informer le Conseil de sécurité que l'Inde a proposé d'organiser prochainement sur son territoire une réunion spéciale du Comité contre le terrorisme, qui sera exclusivement consacrée à cette question et tentera de proposer des solutions.

Deuxièmement, certains États exploitent les compétences qui sont les leurs dans le domaine numérique pour réaliser leurs objectifs politiques et de sécurité et pour se livrer à des formes modernes de terrorisme transfrontalier, pour attaquer des infrastructures nationales critiques, telles que les installations sanitaires et énergétiques, et pour perturber l'harmonie sociale en promouvant la radicalisation par l'intermédiaire de l'espace en ligne. Les sociétés ouvertes se sont révélées particulièrement vulnérables à ces menaces et aux campagnes de désinformation. Les technologies numériques émergentes, par exemple l'utilisation de l'apprentissage automatique et des

mégadonnées, peuvent renforcer la létalité de ces actes, constituant ainsi une grave menace pour la paix et la sécurité internationales. Lorsqu'il s'agit de faire face à ces menaces, la communauté internationale ne peut pas adopter une approche sélective et doit éviter le deux poids, deux mesures.

Troisièmement, la nature interconnectée du domaine numérique fait que nous ne pouvons pas régler les problèmes complexes et nous attaquer aux menaces émanant de ce domaine de manière isolée. Il est essentiel que nous adoptions une approche collaborative fondée sur des règles et que nous nous efforcions d'en garantir l'ouverture, la stabilité et la sécurité. Favoriser un accès équitable aux technologies numériques et à leurs avantages doit également constituer un élément important de cette approche. La fracture numérique qui se creuse, la fracture numérique entre les genres et l'écart des compétences numériques créent un environnement non viable dans le domaine du cyberespace. La dépendance croissante au numérique depuis le déclenchement de la maladie à coronavirus (COVID-19) a exacerbé les risques et mis en lumière ces inégalités face au numérique. Ces problèmes doivent être réglés par le renforcement des capacités et le transfert de technologie.

Quatrièmement, les missions de maintien de la paix des Nations Unies doivent être équipées des technologies numériques les plus récentes pour contrer celles qui sont utilisées par les groupes armés. La protection des protecteurs doit être notre priorité au même titre que la protection des civils. Nous avons agi sur ce front en déployant, en partenariat avec l'ONU, la plateforme Unite Aware pendant notre présidence du Conseil, en août 2021. Ce programme technologique permet aux soldats de la paix d'évaluer les menaces en temps réel et doit être étendu à toutes les missions de maintien de la paix des Nations Unies. Je remercie le représentant de la France d'avoir fait allusion à la déclaration du Président du Conseil de sécurité sur la technologie et le maintien de la paix (S/PRST/2021/17), adoptée sous notre présidence en 2021.

Cinquièmement, le maintien de la paix et de la sécurité internationales dans le cyberespace dépend également de l'échange d'informations entre les pays sur l'utilisation abusive des technologies numériques à des fins criminelles. Cette coopération doit être efficace et se faire en temps réel afin de prévenir cette utilisation abusive, d'y faire obstacle et d'en atténuer les conséquences. Par conséquent, la création 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 est un pas dans la bonne direction.

Pour terminer, qu'il me soit permis de réaffirmer que la communauté mondiale doit tirer parti des technologies numériques dans l'intérêt de l'ensemble de l'humanité et pas seulement de quelques privilégiés. Notre objectif global doit être de mettre ces technologies au service du développement, de la prospérité et de l'autonomisation de tous et de promouvoir la paix et la sécurité internationales. L'Inde est prête à offrir ses compétences et à partager son expérience dans cette entreprise commune.

M. Zhang Jun (Chine) (*parle en chinois*) : Le développement rapide de la science et de la technologie a apporté de nouvelles perspectives et de nouveaux défis. En mai de l'année dernière, la Chine, les Émirats arabes unis, le Kenya et le Mexique ont organisé conjointement une réunion selon la formule Arria pour procéder à un échange de vues approfondi sur les conséquences des technologies émergentes sur la paix et la sécurité internationales. La Chine se félicite de cette occasion de poursuivre le débat sur la technologie et la sécurité au sein du Conseil afin de mieux développer et utiliser la science et la technologie au profit de l'humanité.

La Chine voudrait formuler les propositions suivantes. Premièrement, nous devons promouvoir vigoureusement l'innovation scientifique et technologique. L'innovation est le principal moteur du développement. Toutes les révolutions scientifiques, technologiques et industrielles de l'histoire de l'humanité ont profondément transformé notre mode de production et notre mode de vie, et ont considérablement favorisé le progrès et le bien-être de l'humanité.

Le monde est aujourd'hui confronté à des problèmes complexes et sans précédent. L'évolution rapide des technologies numériques, l'intelligence artificielle et la biotechnologie, entre autres, jouent un rôle important dans les domaines de la prévention et de la maîtrise des pandémies, de la lutte contre les changements climatiques, de la sécurité alimentaire, de la sécurité énergétique et dans d'autres domaines. Qu'il s'agisse de relancer la croissance économique mondiale ou de trouver de nouveaux moyens de régler de grands problèmes complexes, l'innovation dans le domaine des sciences et des technologies est tout simplement indispensable.

L'économie mondiale étant fortement interdépendante et les chaînes industrielles et d'approvisionnement mondiales étroitement interconnectées, tous les pays doivent envisager les échanges internationaux et la coopération dans le domaine des sciences et des technologies dans un esprit d'ouverture et les promouvoir en appliquant les mesures pertinentes, créer ensemble un environnement ouvert, équitable, juste et non discriminatoire à cet égard, et mener conjointement des activités de recherche et de développement pour favoriser le progrès en déployant des efforts concertés.

Deuxièmement, les avancées dans le domaine des sciences et des technologies doivent bénéficier à tout le monde. La technologie ne connaît pas de frontières et fait partie du patrimoine commun de l'humanité. Ces avancées ne doivent pas devenir des trésors cachés dans des caves. À l'heure actuelle, la fracture technologique croissante entre les pays développés et en développement, en particulier la fracture numérique, exacerbe des inégalités nouvelles.

Il faut permettre aux plateformes multilatérales telles que l'ONU de jouer pleinement leur rôle dans le renforcement des capacités de recherche et de développement des pays en développement ; accélérer le transfert des technologies ; accélérer la commercialisation des réalisations scientifiques ; partager les dividendes des progrès dans le domaine des sciences et des technologies avec les pays en développement ; surmonter le déficit de développement en réduisant la fracture numérique ; et accélérer la mise en œuvre du Programme de développement durable à l'horizon 2030.

Il faut aider les pays en développement à utiliser les technologies de pointe et les mégadonnées afin d'améliorer la gouvernance sociale et de prévenir et combattre efficacement la criminalité.

Dans les domaines du maintien et de la consolidation de la paix, le Conseil doit également utiliser activement les nouvelles technologies pour renforcer ses capacités en matière de collecte d'informations, d'alerte rapide, d'interventions d'urgence et de sauvetage.

Troisièmement, il est impératif d'œuvrer de concert pour gérer et maîtriser les risques associés à la technologie. Les avancées techniques peuvent générer des risques liés à des règles contradictoires, des risques sociaux et des problèmes éthiques. La communauté internationale doit défendre le concept de sciences et technologies au service de l'humanité ; permettre à l'ONU de jouer son rôle en tant qu'enceinte principale d'un dialogue, d'échanges et d'une coopération actifs ; adhérer au principe de participation multilatérale et multipartite ; gérer conjointement les risques associés au développement technologique ; et formuler et renforcer des règles et normes universellement acceptées.

Il faut juguler l'utilisation abusive des technologies de l'information et s'opposer à la cybersurveillance, aux cyberattaques et à une course aux armements dans le cyberespace. Il est crucial d'empêcher les terroristes d'utiliser Internet à des fins de recrutement ou pour financer ou organiser des attentats terroristes, mais aussi d'empêcher qu'Internet devienne un vivier de discours de haine, de racisme, de pornographie et de violence. Les gouvernements doivent renforcer la supervision et le contrôle dans le respect des lois, uniformiser l'application des technologies et protéger plus efficacement l'intérêt public. Les fournisseurs d'accès aux plateformes informatiques et les fournisseurs d'accès à Internet doivent uniformiser leurs pratiques et renforcer leur autodiscipline afin d'honorer leurs responsabilités sociales.

Quatrièmement, nous sommes opposés à la politisation des questions à caractère technologique. Le monde des sciences n'est pas un champ de bataille à somme nulle. L'innovation technique ne doit pas produire un champion unique. Il est néanmoins préoccupant que, depuis un certain temps, certains gouvernements politisent les questions de nature scientifique et technique. Ils ont fait une généralité du concept de sécurité nationale, abusé du pouvoir de l'État et intensifié gratuitement la répression des sociétés étrangères spécialisées dans les technologies de pointe. Pour maintenir leur monopole dans le domaine des sciences et des technologies, ces gouvernements ont créé des cercles et des clubs exclusifs en vertu de prétendus stratégies et cadres. Ils imposent des blocus techniques à d'autres pays et ont recours à des pratiques d'intimidation dans le domaine des sciences et des technologies. Ils entravent et obstruent la coopération économique, commerciale, scientifique et technique entre les autres pays.

Cette approche, qui est révélatrice d'une mentalité obsolète datant de la guerre froide, est contraire à l'esprit de la coopération internationale et aux tendances de notre époque. Elle porte atteinte aux intérêts collectifs de tous les pays et elle est vouée à l'échec. Nous exhortons certains gouvernements à adopter une approche rationnelle et ouverte d'esprit ; à adopter la

bonne perspective en ce qui concerne le développement scientifique et technique et la coopération internationale ; et à cesser d'attaquer sans raison les sociétés étrangères spécialisées dans les technologies de pointe et de leur imposer des restrictions infondées.

Face aux défis mondiaux, la voie à suivre est celle de la solidarité et de la coopération. La Chine appelle les pays concernés à cesser de créer des divisions dans le monde entier, notamment dans la région d'Asie et du Pacifique ; à mettre fin à la confrontation géographique ; à cesser de tracer des frontières idéologiques et d'avoir recours à des mesures coercitives pour forcer d'autres pays à prendre parti ; à s'abstenir de dissocier l'économie des sciences et des technologies ; et à mettre fin à leurs pratiques destructrices qui nuisent à la stabilité des chaînes d'approvisionnement mondiales et au relèvement économique.

La Chine attache une grande importance à l'innovation scientifique et technique et lutte contre les risques technologiques de manière responsable. Nous promouvons activement la coopération et le consensus internationaux. En 2020, la Chine a lancé une initiative mondiale pour la sécurité des données, appelant à garantir l'ouverture, la sécurité et la stabilité des chaînes d'approvisionnement mondiales tout en s'opposant à la pratique qui consiste à utiliser les technologies de l'information pour détruire des infrastructures critiques ou mener des activités de surveillance à grande échelle. Elle plaide également pour le respect de la souveraineté et de la juridiction nationales, ainsi que le droit des États à gérer leurs propres données. Cette initiative constitue un modèle pour l'élaboration de règles internationales en matière de sécurité numérique, et nous espérons qu'elle suscitera la participation des gouvernements, des organisations internationales et de multiples parties.

Face aux défis considérables engendrés par l'intelligence artificielle, et à la suite d'années de délibérations à l'ONU, à la fin de l'année dernière, la Chine a présenté un document de position sur la réglementation des applications militaires de l'intelligence artificielle. Celui-ci fournit un cadre viable pour permettre à la communauté internationale d'analyser l'incidence des applications militaires de l'intelligence artificielle sur les règles et normes déontologiques relatives à la gouvernance stratégique du secteur de la sécurité.

En juillet dernier, des scientifiques originaires de plus de 20 pays ont adopté les Directives de sûreté biologique de Tianjin pour l'élaboration de codes de conduite à l'intention des scientifiques, qui promeuvent un comportement responsable en matière de recherche et de développement dans le domaine de la biotechnologie, ce qui est l'aspiration commune de la communauté scientifique internationale. La Chine se félicite que tous les pays et tous les acteurs concernés aient adopté volontairement et promeuvent les Directives de sûreté biologique de Tianjin afin de prévenir l'utilisation abusive de la biotechnologie, de limiter les risques en matière de sûreté biologique et d'encourager l'utilisation de la biotechnologie dans l'intérêt de l'humanité.

L'utilisation des sciences et des technologies à des fins pacifiques et la coopération internationale à cet égard constituent des droits inaliénables de tous les États en vertu du droit international. Durant sa soixante-seizième session, l'Assemblée générale a adopté une résolution intitulée « Promotion de la coopération internationale touchant les utilisations pacifiques dans le contexte de la sécurité internationale » (résolution 76/234). La Chine et 26 autres pays se sont portés coauteurs de cette résolution, qui exhorte tous les pays, sans préjudice de leurs obligations internationales en matière de non-prolifération, à lever les restrictions déraisonnables à l'exercice du droit des pays en développement à utiliser les sciences et les technologies à des fins pacifiques.

La Chine salue la poursuite d'un dialogue inclusif dans le cadre de l'Assemblée générale en vue de renforcer la confiance mutuelle, de générer un consensus et de veiller à ce que les pays en développement jouissent pleinement de leur droit aux utilisations pacifiques des sciences et des technologies. Cela nous permettra d'œuvrer plus efficacement à la réalisation des objectifs de développement durable et au maintien de la paix et de la sécurité internationales.

M. Kiboino (Kenya) (*parle en anglais*) : Je remercie la Secrétaire générale adjointe, M^me^ DiCarlo, ma compatriote M^me^ Nyabola et M. Druet de leurs observations et de leurs recommandations sur la question dont nous sommes saisis aujourd'hui.

Quand on réfléchit au rôle phénoménal que la technologie numérique a joué au cours de cette seule décennie et aux effets sans précédent que la révolution numérique a eus sur la paix et la sécurité de notre temps, et compte tenu du caractère généralisé, conséquent et largement non réglementé des technologies numériques, il devient parfaitement clair qu'il faut une communauté de débatteurs et d'acteurs, dont le Conseil de sécurité, pour examiner l'équilibre délicat entre la nécessité de garantir l'innovation numérique, d'une part, et

d'empêcher son utilisation malfaisante par des acteurs tant étatiques que non étatiques dans des aspects touchant la paix et la sécurité, d'autre part.

Le Kenya a déjà beaucoup fait pour garantir l'accessibilité d'Internet et que le pays et ses citoyens soient protégés autant que possible des perturbations, des événements inattendus et des menaces survenant dans la sphère numérique. Toutefois, nous sommes conscients que la cybersécurité n'est pas et ne peut pas être l'affaire d'un seul pays. En effet, la quête conventionnelle de la paix et de la sécurité internationales par le système multilatéral doit maintenant être entreprise dans le domaine cybernétique.

À cet égard, je mettrai l'accent sur cinq points à examiner. Mon premier point concerne la nécessité de comprendre que l'ONU devrait aider les pays à gérer les conséquences de la révolution numérique sur leurs citoyens et leur stabilité nationale, y compris le détournement de l'intelligence artificielle, les mégadonnées, les médias sociaux et d'autres frontières numériques. Le Conseil de sécurité a la responsabilité de veiller à ce que l'ONU ait les capacités et les compétences spécialisées requises pour jouer ce rôle.

Mon deuxième point a trait au lien entre les technologies numériques et la paix, en particulier dans les transitions politiques. Les processus électoraux sont une promesse démocratique, mais ils sont souvent confrontés à de plus grandes vulnérabilités en matière de sécurité sur les plateformes numériques, ce qui a des répercussions sur la cohésion civique et la gestion de crise à l'échelle nationale. Le 28 octobre 2021, durant notre présidence du Conseil de sécurité, le Kenya a convoqué une réunion organisée suivant la formule Arria sur les moyens de traiter et de contrer les discours de haine et d'empêcher l'incitation à la discrimination, à l'hostilité et à la violence sur les médias sociaux. Il est évident que les décideurs sont souvent face à un dilemme pour trouver un équilibre entre la liberté d'expression et les discours de haine et entre la responsabilité démocratique et la préservation des informations privées et protégées. Nous plaidons pour plus d'attention et d'investissement au profit des gouvernements nationaux afin de les aider à s'occuper du lien entre la cybersécurité et leur sécurité électorale, en particulier dans les situations de conflit.

Mon troisième point se rapporte aux partenariats entre le secteur privé et les instances de réglementation. La réunion organisée suivant la formule Arria, que je viens de mentionner, a rassemblé des représentants d'entreprises de technologie, dont Facebook, Twitter, TikTok et Google, et de la société civile, qui ont démontré qu'il était possible d'établir de tels partenariats. Des partenariats renforcés entre les entreprises de technologie, les instances de réglementation et l'ONU permettront de mettre en place des mécanismes et des normes efficaces pour garantir un comportement responsable dans le cyberespace, sur la base de principes qui abordent le bien public de manière à jeter des ponts de paix entre divers groupes et en ce qui concerne tous les thèmes clivants.

Mon quatrième point porte sur le lien entre les technologies numériques et le terrorisme. La nature généralisée, programmable et axée sur les données des nouvelles technologies, bien que profitable, a ouvert la voie à leur détournement par des groupes armés et des terroristes. Ils tirent avantage de systèmes à l'interface simplifiée pour recruter, radicaliser, mobiliser des ressources et planifier et mettre à exécution des actes de terrorisme. Il faut s'assurer que les États aient les capacités nécessaires pour atténuer la menace terroriste en ligne, rehausser leurs compétences en matière d'enquêtes et collaborer à la réduction du taux de radicalisation en ligne et des flux financiers illicites et à l'identification et la suppression des contenus extrémistes en ligne.

Mon cinquième point concerne l'inclusion et la protection de la participation. Nous estimons que la responsabilité gouvernementale en matière d'accessibilité d'Internet inclut aussi la protection des personnes qui accèdent aux plateformes numériques, y compris les médias sociaux. En particulier, la sécurité des femmes participant à des processus de paix et de sécurité demeure cruciale. Les États doivent donc renforcer l'application du principe de responsabilité et les poursuites contre les auteurs d'attaques et de manœuvres d'intimidation en ligne, ceux qui publient des contenus privés et les individus coupables de violence physique contre des femmes participant au programme de paix. Dans le cadre de la préservation des piliers de protection et de participation du programme pour les femmes et la paix et la sécurité, le Conseil de sécurité devrait également prendre des mesures précises, en particulier afin d'accroître le prix à payer pour toutes les formes d'intimidation en ligne contre des femmes ayant fait des exposés au Conseil.

M. Gómez Robledo Verduzco (Mexique) (*parle en espagnol*) : En premier lieu, nous tenons à vous remercier, Madame la Présidente, d'avoir convoqué la présente séance sur un thème aux ramifications presque

infinies qui nous engage à réfléchir, entre autres, à la manière d'adapter le travail de l'ONU pour surmonter les problèmes posés par l'utilisation de la technologie numérique en ce qui concerne le maintien de la paix et de la sécurité internationales. Nous sommes également reconnaissants aux intervenants de ce matin, la Secrétaire générale adjointe DiCarlo, la Directrice d'Advox et le Professeur Druet, de l'Université McGill, de leurs excellentes analyses et propositions.

Si nous regardons les choses en face, nous devons partir du principe que la technologie numérique doit d'abord et avant tout être utilisée pour défendre les droits humains et la démocratie. Les deux aspects sont indissociables. À cet égard, le Mexique réaffirme son attachement, qu'il a maintenu au fil des années, à un cyberespace libre, ouvert et sûr, où le droit international, y compris le droit international des droits de l'homme, le droit international humanitaire, le droit pénal international et d'autres précédents juridiques établissant par exemple le droit à la vie privée, s'applique pleinement. Nous rappelons les accords que nous avons déjà conclus et qui sont en vigueur au niveau intergouvernemental, en particulier dans le domaine de la cybersécurité, par l'intermédiaire des rapports du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation. De même, il nous incombe de rappeler d'autres processus en cours, notamment 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.

Il faut chercher des solutions novatrices aux problèmes actuels dans le domaine du maintien de la paix, en particulier par le renforcement des capacités numériques des opérations de paix et des missions politiques spéciales, comme mentionné plus tôt dans les exposés d'aujourd'hui. L'utilisation de la technologie peut contribuer de manière très constructive à l'amélioration de la détection rapide des menaces naissantes, à la prévention des crises humanitaires et des violations des droits humains et au renforcement des mesures nécessaires pour protéger et appuyer les civils et les infrastructures civiles, y compris dans la lutte contre le trafic d'armes et dans les activités de déminage.

Les nouvelles technologies sont particulièrement prometteuses dans des domaines comme l'assistance médicale, notamment la fourniture de soins psychosociaux et de santé mentale de routine et d'urgence. Les soldats de la paix et les civils touchés par les crises humanitaires peuvent profiter de la souplesse et de l'accessibilité offertes par la télémédecine. En outre, nous voyons que l'utilisation de technologies relatives aux énergies renouvelables peut améliorer la sûreté et la sécurité du personnel des Nations Unies et l'efficacité et la viabilité des missions. Face à la désinformation croissante, soulignée précédemment, l'utilisation des réseaux sociaux est cruciale pour renforcer les relations entre les missions de maintien de la paix et les communautés au sein desquelles elles opèrent. C'est pourquoi les dispositions de la résolution 2589 (2021) et de la déclaration du Président S/PRST/2021/17, dans lesquelles le Conseil de sécurité a reconnu que la technologie pouvait aider les missions de maintien de la paix à mieux comprendre les contextes dans lesquels elles opèrent, sont absolument indispensables et doivent nous permettre d'améliorer la manière dont nous recueillons, analysons et partageons les informations.

De même, nous prenons note de la Stratégie pour la transformation numérique du maintien de la paix des Nations Unies en ce qui concerne les nouvelles technologies et les données, qui fait suite à l'initiative Action pour le maintien de la paix Plus. La mise en œuvre de cette stratégie requiert une coordination accrue entre le système des Nations Unies et les parties prenantes sur le terrain, ainsi qu'une coopération avec les organisations régionales, le secteur privé, les organisations de la société civile et, bien sûr, les universités.

À la dernière Conférence ministérielle des Nations Unies sur le maintien de la paix, le Mexique a souscrit à l'initiative présentée par la République de Corée sur la technologie et le renforcement des capacités médicales dans le domaine du maintien de la paix. Cette initiative a trois objectifs : optimiser l'utilisation des technologies disponibles pour une meilleure appréciation de la situation et l'alerte rapide ; réagir à la désinformation dans les situations de conflit et améliorer les renseignements dans le domaine de la cybersécurité ; et promouvoir le renforcement des capacités dans le domaine de l'analyse des données et des informations.

Enfin, la résolution 75/316, promue par le Mexique à l'Assemblée générale, met en exergue l'incidence de l'évolution rapide de la technique sur la réalisation du Programme de développement durable à l'horizon 2030 et, par conséquent, sur la paix et la stabilité internationales. Nous soulignons l'importance du Plan d'action de coopération numérique et des informations contenues dans le rapport *Notre Programme commun* (A/75/982).

M. Agyeman (Ghana) (*parle en anglais*) : Pour commencer, je remercie les États-Unis d'avoir organisé la présente séance d'information sur l'utilisation des technologies numériques dans le cadre du maintien de la paix et de la sécurité internationales.

Je remercie également la Secrétaire générale adjointe Rosemary DiCarlo de son exposé instructif, ainsi que Nanjala Nyabola, Directrice d'Advox, projet de Global Voices dédié aux droits numériques, et Dirk Druet, chargé d'enseignement au Centre d'études sur la paix et la sécurité internationales de l'Université McGill, de leurs observations complémentaires.

Étant donné l'omniprésence des technologies numériques dans le monde, le Ghana partage l'avis que celles-ci peuvent jouer un rôle important dans le maintien de la paix internationale et doivent donc être utilisées pour renforcer la sécurité collective. Nous pensons que, compte tenu des exigences liés à la souveraineté nationale et à l'intégrité territoriale, les technologies numériques, qui permettent de surmonter les barrières territoriales, peuvent être utilisées pour renforcer les objectifs de la diplomatie préventive grâce à une meilleure appréciation de la situation, lancer des alertes rapides, détecter des menaces émergentes et réduire les divisions au sein de la société en mobilisant différentes opinions et positions en un ensemble constructif et cohérent pour renforcer les objectifs de paix.

Dans le cadre de la gestion des conflits, nous relevons également les avantages que les technologies numériques peuvent apporter à l'analyse des risques et à l'amélioration des délais nécessaires à la protection des civils et des infrastructures civiles, sans oublier la rigueur qu'elles procurent et qui permet de mieux défendre les mandats des opérations de soutien à la paix et de renforcer la sûreté et la sécurité des personnels en tenue et autres. Les technologies numériques peuvent aussi apporter un solide appui aux efforts de consolidation de la paix et de reconstruction de sociétés détruites par la guerre.

Le Ghana est convaincu que si nous voulons tirer le meilleur parti des avantages incommensurables qu'offrent les technologies numériques en matière d'intensification des efforts de maintien de la paix et de la sécurité internationales, nous avons besoin d'un consensus sur le cadre normatif qui sous-tend cette approche améliorée et complémentaire de l'utilisation des outils modernes disponibles au service de la paix dans le monde. En effet, nous sommes bien conscients du fait qu'en dépit de leur caractère inoffensif, les technologies numériques peuvent également exacerber l'insécurité internationale si elles ne sont pas utilisées de manière responsable. Elles peuvent renforcer la méfiance dans des sociétés fragiles et soumises à des tensions s'il existe un sentiment persistant que des forces extérieures manipulent la volonté de la population pour lui faire adopter des valeurs qui seraient étrangères à ces sociétés.

Nous relevons également la malveillance avec laquelle les technologies numériques ont été utilisées dans certains cas par des acteurs étatiques et non étatiques pour désinformer et manipuler les populations, menacer et harceler personnellement des militants et des journalistes et alimenter les discriminations afin de nuire à l'unité et à la cohésion nationales. Il est également préoccupant de voir la manière dont ces technologies sont utilisées pour radicaliser des personnes et les recruter dans des groupes terroristes, organiser des attaques terroristes et financer des activités terroristes.

Sachant le potentiel immense que recèlent les technologies numériques pour renforcer les outils existants de maintien de la paix et de la sécurité internationales, tout en étant conscients de leurs conséquences négatives, nous souhaitons souligner quelques points supplémentaires. Comme indiqué précédemment, l'utilisation des technologies numériques dans le maintien de la paix et de la sécurité internationales doit se faire à partir d'un point de convergence et sur la base de principes qui respectent la souveraineté nationale et promeuvent les valeurs universelles. À cet égard, nous pensons que l'ONU a un rôle indispensable à jouer pour renforcer l'incidence positive des technologies numériques sur la paix dans le monde. Par exemple, en s'appuyant sur les engagements pris dans la Stratégie pour la transformation numérique du maintien de la paix des Nations Unies, lancée par le Secrétaire général, qui vise à saisir les possibilités offertes par les technologies numériques, les missions pourront s'adapter à l'évolution de la dynamique d'un conflit et bénéficier d'une efficacité accrue. En outre, les enseignements que le Département des affaires politiques et de la consolidation de la paix a tirés des efforts de médiation déployés pendant la pandémie de maladie à coronavirus (COVID-19) via les technologies numériques peuvent être utiles pour élaborer des cadres durables permettant d'échanger avec l'ensemble de la population afin de parvenir à la paix.

Deuxièmement, la capacité des gouvernements nationaux d'améliorer leur espace de cybersécurité doit être au cœur de l'élaboration d'un cadre solide pour

l'utilisation des technologies numériques. En raison de l'utilisation malveillante des technologies numériques par les terroristes et les groupes extrémistes et la tendance à la cyberguerre, les pays vulnérables, comme certains pays d'Afrique où des fragilités existent, doivent obtenir l'appui nécessaire pour renforcer leurs capacités numériques, conformément à la Stratégie de *transformation* numérique pour l'Afrique (2020-2030) de l'Union africaine. Ces efforts de renforcement des capacités doivent inclure la collecte, le traitement, l'utilisation et l'analyse des nouvelles technologies et de leur incidence sur la sécurité. À cet égard, l'appui offert par la Direction exécutive du Comité contre le terrorisme est louable, et nous nous félicitons des autres efforts de ce type.

Troisièmement, les États ont aussi un rôle essentiel à jouer en adoptant des politiques qui préviennent l'utilisation abusive du cyberespace grâce à des éléments qui, entre autres, stimulent les investissements dans les infrastructures nationales critiques, promeuvent des contenus médiatiques responsables et facilitent la détection rapide, les enquêtes et les poursuites judiciaires des contrevenants. Les États doivent honorer les engagements pris en vertu de la Charte des Nations Unies en respectant le droit international des droits de l'homme de manière à garantir que les données personnelles collectées, stockées, traitées, utilisées, transférées et divulguées respectent et protègent la vie privée des personnes. En outre, nous saluons les mesures qui encouragent les entreprises à respecter le droit international des droits de l'homme et les normes commerciales en la matière, sur la base des Principes directeurs relatifs aux entreprises et aux droits de l'homme.

Quatrièmement, conscients de l'efficacité des accords régionaux en matière de prévention des conflits grâce à des mécanismes d'alerte rapide et de consolidation de la paix dans les situations post-conflit, nous recommandons instamment le renforcement des partenariats axés sur les technologies numériques entre les systèmes multilatéraux internationaux et les organismes régionaux. Nous préconisons d'appuyer l'application des traités existants, tels que la Convention de Budapest et la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, également connue sous le nom de Convention de Malabo, et considérons que les mécanismes d'alerte rapide, tels que ceux de la Communauté économique des États de l'Afrique de l'Ouest et de l'Union africaine, peuvent être renforcés grâce à un appui ferme de la communauté internationale.

En outre, le soutien aux plateformes régionales de partage de renseignements et d'informations pourrait améliorer la détection rapide des visées expansionnistes des réseaux terroristes, notamment en Afrique de l'Ouest et en ligne. Par ailleurs, les mesures visant à tarir le financement du terrorisme doivent être appuyées et renforcées, y compris dans l'économie virtuelle, où les cryptomonnaies sont devenues le moyen de prédilection pour financer les activités terroristes. Même si la collaboration entre le Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest et les centres nationaux de renseignement financier d'Afrique de l'Ouest a permis d'obtenir de bons résultats, ses actions doivent encore être approfondies.

Avant de terminer, je voudrais souligner la détermination du Ghana à améliorer l'utilisation des technologies à des fins pacifiques grâce aux mesures qui ont été prises pour renforcer l'écosystème national des technologies de l'information et des communications. Outre l'institutionnalisation d'un mois national de sensibilisation à la cybersécurité visant à mieux informer l'ensemble de la société sur les cybermenaces, la mise en place d'équipes sectorielles d'intervention informatique d'urgence au sein d'institutions clefs, telles que l'Autorité nationale des communications, la Banque centrale et l'Agence nationale des technologies de l'information, a permis de renforcer la résilience du cyberécosystème pour tous les services en ligne, le secteur financier et les entreprises publiques. Nous préconisons donc une approche mobilisant l'ensemble de la société pour développer la résilience dans le cadre du lien entre paix et sécurité, y compris des partenariats avec le secteur privé, les organisations de la société civile et les géants de la technologie, dont le rôle croissant doit être mis au service du bien public. Par ailleurs, les femmes et les jeunes sont des agents essentiels du changement et continueront de jouer un rôle essentiel pour renforcer l'incidence positive des technologies sur la sécurité mondiale.

Le Ghana est attaché à l'objectif collectif d'améliorer tous les outils disponibles et estime que les initiatives multilatérales et régionales peuvent exploiter efficacement les technologies pour atteindre les objectifs de paix et de sécurité mondiales.

M. Nebenzia (Fédération de Russie) (*parle en russe*) : Nous remercions les intervenants de leurs exposés.

Les technologies numériques ont transformé le monde et font désormais partie intégrante de ses processus économiques, politiques et sociaux. On espérait

qu'elles deviendraient un moteur du progrès économique et social, qu'elles faciliteraient les communications et aideraient l'humanité à passer à un nouveau stade de développement numérique.

Pendant la pandémie de maladie à coronavirus (COVID-19), les technologies de l'information et des communications (TIC) ont permis de préserver les emplois et l'unité de notre monde fragmenté par les mesures de quarantaine. Les TIC sont devenues pratiquement l'élément vital des services publics fournis par les gouvernements, y compris des travaux des hôpitaux, des banques et du secteur financier en général, des écoles et d'autres institutions essentielles de la société. Il n'est pas exagéré de dire que l'humanité n'a jamais été aussi dépendante des TIC qu'aujourd'hui.

Mais les espoirs de voir les TIC devenir une force exclusivement au service du bien ne se sont pas concrétisés. Le coupable n'est pas la technologie, mais le fait qu'elle a été utilisée pour atteindre des objectifs géopolitiques et pour imposer l'hégémonie, non seulement dans le monde physique, mais aussi en ligne.

Ces dernières années, la manipulation de l'information a pris des proportions alarmantes. Toute une armée de pseudo-enquêteurs issus d'organisations non gouvernementales a vu le jour et, à la demande des gouvernements occidentaux, produit des soi-disant enquêtes biaisées qui, en fait, génèrent et diffusent de nombreux mensonges et des informations non corroborées provenant de sources en accès libre afin de ternir la réputation des pays qui dérangent l'Occident. Les Casques blancs et Bellingcat en sont des exemples notoires. Ils se sont distingués en diffusant des mensonges grossiers dans l'intérêt de la propagande occidentale sur le dossier chimique syrien, l'incident du vol MH-17 de la Malaysia Airlines et de nombreuses autres questions très médiatisées. Les experts les ont pris en flagrant délit, pour ainsi dire, à plusieurs reprises, en soulignant les incohérences de leurs conclusions, qui n'ont rien à voir avec un journalisme d'investigation professionnel et indépendant et qui ont été formulées en violation de tous les principes les plus fondamentaux.

Une nouvelle tendance très préoccupante se dessine : une guerre de l'information est menée non seulement d'une manière totalement éloignée de la réalité, mais également dans le but de déformer la réalité, voire de la remplacer complètement. La vérité est supplantée par un flot continu d'informations et de spams à caractère idéologique, afin de ne pas donner au public la moindre chance d'avoir une vision objective des faits.

Un exemple flagrant est l'incident concernant la mort de civils à Boutcha, au sujet duquel des informations ont été diffusées par les médias occidentaux à la demande de leurs gouvernements, en accusant l'armée russe. Ils ont fait abstraction de tous les faits et des éléments de preuve objectifs pour diffuser des mensonges. Sous la pression des faits, même les médias occidentaux ont finalement été contraints d'admettre que les paisibles habitants de Boutcha n'étaient pas morts de blessures par balle, mais qu'ils avaient été tués par des obus d'artillerie obsolètes utilisés par les forces armées ukrainiennes lorsqu'elles ont bombardé la ville. Ils lancent maintenant de nouvelles accusations inventées de toutes pièces pour détourner l'attention de la responsabilité évidente de l'armée ukrainienne dans cet acte de provocation de Boutcha. De même, les médias occidentaux préfèrent ne plus mentionner les attaques contre Kramatorsk après l'apparition de preuves claires de l'implication des forces armées ukrainiennes.

Ces derniers mois, les travaux du ministère occidental de la vérité, ou plus exactement du ministère du mensonge, ont atteint un point culminant. Une campagne de désinformation et de manipulation de l'opinion publique sans précédent par son ampleur et son intensité a été déclenchée contre la Russie. Les médias occidentaux, qui n'étaient déjà pas connus pour leur objectivité, se sont finalement transformés en porte-voix d'une propagande d'État grossière et en usine à fausses nouvelles.

Les géants des TIC, qui ont monopolisé la sphère des réseaux sociaux et de l'hébergement vidéo, ne se comportent pas mieux. Les plateformes numériques ont enfin jeté les masques et ne cherchent plus à cacher leur parti pris politique. Elles bloquent tous les comptes dont le contenu ne correspond pas au programme dicté par les élites occidentales. La société Meta a explicitement autorisé les discours de haine et les appels à la violence contre les Russes et les russophones sur ses plateformes.

Des États qui se qualifient de « communauté des démocraties » sont en fait les artisans d'un véritable cyber-totalitarisme. Ils veulent créer un monde dans lequel eux seuls auront le contrôle total des flux d'information et détermineront ce qui est vrai et ce que le public doit lire et voir. Tout point de vue alternatif est immédiatement qualifié de désinformation et de propagande, et les faits gênants sont écartés. Des chaînes de télévision russes sont fermées, des journalistes russes sont expulsés et l'accès à des sites Web russes est bloqué. Est-ce cela la prétendue liberté d'accès à l'information ?

Nous espérons que c'est ce que les organisateurs de la présente séance entendaient par abus des restrictions d'accès aux ressources Internet sous le prétexte de garantir la sécurité nationale.

La campagne d'information russophobe menée par ses initiateurs vise divers domaines d'activité, y compris ceux qui n'ont aucun lien avec la politique, comme l'éducation, la culture et le sport. Il s'agit d'une violation flagrante du principe fondamental de la non-discrimination fondée sur l'appartenance ethnique. Outre l'agression informationnelle qui cible les esprits, une campagne a été lancée pour saper l'infrastructure TIC elle-même par le biais d'attaques informatiques. Kiev a récemment annoncée la création d'une cyberarmée et a ouvertement admis avoir mené des cyberattaques contre des cibles russes et bélarussiennes. De plus, les parrains occidentaux du régime de Kiev non seulement n'ont pas essayé de les empêcher, mais ils entretiennent délibérément cette armée de hackers, sans penser aux conséquences. Comme nous le savons, l'OTAN a récemment mené des activités en ce sens dans le cadre de l'exercice de cybersécurité Locked Shields, auquel participent les forces armées ukrainiennes.

En avril, Washington a annoncé une récompense de 10 millions de dollars pour quiconque pourrait prouver la théorie selon laquelle les services de renseignement russes seraient impliqués dans des cyberattaques contre les États-Unis. Nos appels répétés pour que les organismes compétents traitent ces questions sont restés lettre morte.

Les gouvernements occidentaux font délibérément appel à des groupes de pirates informatiques, voire même à des utilisateurs ordinaires, pour organiser des cyberattaques. Ils diffusent dans le domaine public des informations sur des outils spéciaux et des instructions détaillées sur la manière de lancer des cyberattaques. Sur les médias sociaux, ils font campagne pour que des attaques de pirates informatiques soient menées contre les infrastructures russes.

Dans ce contexte, nous n'avons pas été surpris d'apprendre que Nina Yankovic, qui est née dans l'ouest de l'Ukraine, avait été nommée à la tête du « Conseil de gouvernance de la désinformation » du Département de la sécurité intérieure des États-Unis, créé le 27 avril dernier. M^me^ Yankovic est connue pour avoir mené une campagne d'information visant à blanchir le néonazisme en Ukraine et à diffuser des informations sur le « Russiagate », qui n'a jamais existé. Nous venons d'apprendre qu'elle avait agi ainsi après avoir reçu des instructions directes de l'adversaire de Trump à l'élection présidentielle, Hillary Clinton. Ce cynisme flagrant a fait scandale aux États-Unis même. M^me^ Yankovic a dû démissionner, et le projet a été mis en attente. Nous ne doutons cependant pas qu'il sera relancé sous une forme ou une autre, car nos collègues occidentaux semblent être à court de méthodes diplomatiques. Il ne leur reste que les fausses informations et la désinformation.

Aujourd'hui, l'Ukraine est abreuvée d'armes classiques. Parallèlement, nous assistons à une distribution incontrôlée de cyberarmes et au partage des connaissances sur leur utilisation. Un très grand nombre de personnes acquièrent des compétences pratiques dans ce domaine. Selon Zelenskyy, sa « cyberarmée » compte plus de 300 000 « combattants ».

Les États Membres sont en train de créer une cyberarmée incontrôlable qui se perfectionne sous leur commandement en Ukraine en attaquant la Russie, mais elle ne s'arrêtera pas là. Il ne s'agit pas d'une armée ordinaire. Les experts ne savent que trop bien à quel point il est difficile de suivre les activités des pirates informatiques, d'en identifier la source et d'y mettre un terme. Les pirates informatiques mobilisés par les États Membres se déploieront dans le monde entier, constituant une menace pour les citoyens des pays occidentaux, entre autres.

L'Occident militarise le domaine numérique, ce qui accroît la menace d'un affrontement armé direct, d'autant plus que le régime de Kiev s'inspire activement des méthodes occidentales et maîtrise l'art de la provocation dans la sphère de l'information. Toutefois, leurs conséquences pourraient être encore plus dévastatrices. Les cyberattaques dirigées contre des infrastructures critiques peuvent entraîner des pertes humaines réelles à grande échelle, sans parler du risque de perception erronée en cas d'attaques sous fausse bannière, qui sont beaucoup plus faciles à organiser en ligne que dans le monde réel. Dans ce cas, les risques d'escalade involontaire et de cyberattaques mutuelles augmenteraient de manière exponentielle.

Les actes irréfléchis du régime de Kiev pourraient conduire à un véritable affrontement dans le cyberespace qui impliquerait d'autres pays. L'OTAN a déjà étendu à la sphère de l'information le droit à la légitime défense collective prévu à l'article 5 de son traité. La responsabilité d'une telle escalade incomberait entièrement aux pays occidentaux, qui encouragent le comportement irresponsable de Kiev.

Face à une telle menace, nous ne manquerons pas de riposter à toute tentative de porter atteinte à la sécurité informatique de la Russie. Mais je demande une fois de plus aux membres du Conseil de sécurité de réfléchir au danger que représenterait le fait d'entraîner le monde dans un cyberaffrontement, qui n'est pas moins dangereux que l'utilisation d'armes de destruction massive. Nous essayons d'empêcher un tel scénario de se produire depuis plus de 20 ans déjà.

Je tiens à rappeler que la Russie a été la première à soulever la question de la sécurité internationale de l'information à l'ONU en 1998 et à la faire inscrire à son ordre du jour de manière permanente. C'est nous qui avons insisté pour que l'ONU crée des plateformes de négociation, d'abord réservées aux experts, puis ouvertes à tous les États Membres. À chacune de ces étapes, nous nous sommes heurtés à la résistance farouche de nos collègues occidentaux, qui affirmaient pouvoir se débrouiller sans l'ONU. Le monde ne sait que trop bien comment ils se débrouillent sans l'ONU.

Notre objectif est de faire en sorte que tous les États s'engagent au niveau international à ne pas utiliser les TIC à des fins militaires. Nous exigeons la démilitarisation de la sphère de l'information. Pendant toutes ces années, nous avons proposé des projets d'instruments internationaux spécifiques, un concept universel pour assurer la sécurité internationale de l'information et, au nom de l'Organisation de Shanghai pour la coopération, un projet de code de conduite responsable dans ce domaine.

Qu'ont fait nos collègues occidentaux ? Pendant toutes ces années, ils ont renforcé leurs capacités cybernétiques offensives et élaboré des règles pour les utiliser. Il suffit de rappeler le cynique *Manuel de Tallinn sur le droit international applicable à la cyberguerre*, qui réglemente en détail la manière de mener une cyberguerre dite « humaine ».

Alors, lequel d'entre nous s'est préparé à une cyberguerre pendant toutes ces années ? La Russie, qui a demandé l'interdiction de l'utilisation des TIC à des fins politico-militaires et qui est prête à assumer les obligations correspondantes, ou les pays occidentaux, qui ont rejeté à maintes reprises toutes ces initiatives afin de pouvoir agir à leur guise dans la sphère de l'information ?

Le domaine numérique ne doit pas devenir le théâtre d'affrontements géopolitiques. Il s'agit là d'une question existentielle pour l'humanité. Aujourd'hui, plus que jamais, nous avons besoin d'un dialogue professionnel visant à élaborer des solutions pratiques. Il est de notre devoir de l'appuyer, quel que soit le climat politique. Nous demandons qu'un débat dépolitisé sur tous les aspects de la sécurité internationale de l'information soit organisé dans un forum spécialisé, sous les auspices de l'Assemblée générale : je veux parler du Groupe de travail à composition non limitée. Nous considérons que la présente séance du Conseil ne remplace en aucun cas les activités de ce groupe.

M^me^ Nusseibeh (Émirats arabes unis) (*parle en anglais*) : Les Émirats arabes unis tiennent à remercier les États-Unis d'avoir organisé la présente séance sur une question qui continue de gagner en importance et que les membres du Conseil de sécurité doivent aborder ensemble, indépendamment de leurs différends et en tant que thématique à part entière, selon nous. Nous remercions également la Secrétaire générale adjointe DiCarlo, M^me^ Nyabola et M. Druet de leurs exposés très instructifs d'aujourd'hui.

Les technologies numériques évoluent à une vitesse vertigineuse. Souvenons-nous de l'année 1989, lorsque le World Wide Web a vu le jour. À la fin de la décennie suivante, Larry Page et Sergey Brin ont inventé Google. Nous étions loin de nous douter à l'époque que cette nouvelle idée, née dans un garage en Californie, allait changer nos vies à jamais. Dix ans plus tard, Google était installé sur tous les smartphones et constituait un élément indispensable du travail et de la vie des personnes, apportant d'énormes progrès et changements.

Imaginons maintenant que les effets néfastes de la technologie se propagent aujourd'hui à cette même vitesse vertigineuse et sous nos yeux, comme nous l'avons entendu. Par exemple, les progrès constants des technologies numériques multiplient les capacités des appareils comme les drones. Dans un avenir proche, des essaims de drones, utilisés par des groupes terroristes, pourraient mener des attaques transfrontières, en utilisant la technologie de reconnaissance faciale et d'autres fonctionnalités offertes par l'intelligence artificielle, sans qu'il soit possible de déterminer si ces attaques sont le fait d'un État ou d'un groupe non étatique. Comment les États, y compris ceux représentés autour de cette table, répondront-ils à l'avenir à de telles attaques, dans le respect de la loi et du droit international humanitaire ?

Pour éviter ce futur dystopique, nous devons dès maintenant prendre des mesures urgentes à l'ONU, au Conseil de sécurité et dans d'autres instances. Ce qui

est clair, c'est que nous ne devons pas nous attendre à ce que des réponses constructives émergent des débats politiques et éthiques houleux qui sont menés depuis plus de 20 ans et ne suivent pas le rythme des technologies qui sont désormais omniprésentes et peuvent être utilisées de manière aussi destructrice.

Il ne fait aucun doute que les technologies numériques ont leur lot de risques et de problèmes, notamment en tant que multiplicateur de force pour les groupes terroristes. Toutefois, comme nous l'avons également entendu, ce n'est pas tout.

Les technologies numériques peuvent aussi être des catalyseurs de paix, comme nous l'avons entendu aujourd'hui. Par exemple, les systèmes d'alerte en cas de catastrophe naturelle, qui s'appuient sur les technologies et les données les plus récentes, nous permettent de prévoir les phénomènes météorologiques extrêmes, tels que les sécheresses, les ouragans et les inondations, et de prépositionner les secours en conséquence. Plusieurs programmes d'action préventive en Somalie ont aidé les communautés à faire face aux pénuries d'eau et aux sécheresses dévastatrices. Grâce à ces technologies, le Bureau de la coordination des affaires humanitaires et d'autres partenaires ont pu limiter les pertes de moyens de subsistance et la baisse de la consommation alimentaire, assurer l'accès à l'eau et permettre aux enfants de rester à l'école, comme il se doit. Les informations idoines permettent à la communauté internationale de mieux faire face aux menaces qui pèsent sur la sécurité climatique. Elles permettent de sauver des vies et d'éviter que la fragilité ne devienne un facteur d'instabilité.

Alors que nous examinons la double nature des technologies numériques, il est temps pour le Conseil de ne plus se contenter d'adopter une attitude contemplative face à ce problème et de discuter des moyens concrets par lesquels il peut tirer parti des innovations technologiques pour contribuer à une paix et une sécurité durables. Aujourd'hui, les Émirats arabes unis voudraient aborder cinq questions spécifiques.

Premièrement, comme d'autres l'ont évoqué, il ne faut pas permettre aux groupes terroristes et extrémistes tels que Daech, Al-Qaida et bien d'autres d'utiliser Internet pour propager leurs idées et manipuler les médias sociaux et leurs milliards d'utilisateurs. Les sociétés spécialisées dans les technologies investissent de plus en plus dans des outils de détection basés sur l'intelligence artificielle et dans des équipes de modérateurs humains afin de retirer ces contenus de leurs plateformes. Cependant, il est clair pour les gouvernements depuis un certain temps que les mesures en place ne suffisent pas, car les terroristes et les extrémistes continuent de radicaliser des individus et de les recruter en ligne. Ce problème n'est nullement limité aux pays en développement. Les auteurs d'un certain nombre de crimes haineux récents et très médiatisés contre des minorités religieuses et ethniques dans une grande partie de l'Europe et des États-Unis ont été radicalisés sur ces plateformes en ligne, tout comme d'innombrables recrues de Daech dans le monde. Ainsi, bien que ces dernières années, nous ayons constaté des progrès dans le renforcement des cadres réglementaires et législatifs visant à protéger les utilisateurs contre les contenus terroristes et extrémistes, nous devons évidemment accélérer ces efforts, car le cadre normatif international n'est pas à jour. Cette responsabilité incombe non seulement aux sociétés spécialisées dans les technologies, mais aussi aux gouvernements.

Deuxièmement, nous devons remédier aux effets néfastes des campagnes de désinformation et de mésinformation en ligne qui utilisent les plateformes de médias sociaux, notamment sur les opérations de paix et les activités humanitaires. Ces dernières doivent être protégées. Nous avons vu des cas où les soldats de la paix et les travailleurs humanitaires, qui prennent déjà des risques pour protéger les civils, deviennent encore plus menacés en raison de la diffusion d'informations fausses et trompeuses les visant. Des réponses efficaces pour lutter contre la désinformation sont nécessaires à de nombreux niveaux, notamment par le recours au secteur privé via des règles et des réglementations, la vérification des faits, l'étiquetage des informations et les campagnes d'éducation relatives aux médias. Il convient d'accueillir favorablement les suggestions faites aujourd'hui par les intervenants, à savoir que l'ONU doit renforcer ses capacités et ses compétences à cet égard.

Troisièmement, nous devons tirer parti des technologies numériques pour renforcer la protection des civils. Par exemple, dans le monde physique, les acteurs médicaux et certains acteurs humanitaires utilisent les emblèmes de la croix rouge ou du croissant rouge pour indiquer qu'ils font l'objet d'une protection particulière au titre du droit international humanitaire. Étant donné que ces acteurs sont confrontés à de nouvelles menaces numériques dues à des attaques contre leurs réseaux numériques, nous devons commencer à réfléchir à la possibilité de créer un emblème numérique pour signaler clairement que les acteurs médicaux et humanitaires

ne doivent jamais être pris pour cible, ni en ligne, ni hors ligne. Cet emblème devrait renforcer l'idée selon laquelle ces réseaux doivent être protégés, mais également l'idée selon laquelle tout auteur de violations devra en répondre et selon laquelle le droit international s'applique dans ce domaine.

Quatrièmement, l'innovation numérique a des répercussions sur le monde physique, en multipliant les possibilités d'action des appareils tels que les drones. J'en ai parlé au début de mon intervention. Les drones disponibles dans le commerce peuvent désormais voler plus vite, se déplacer plus loin, transporter des charges utiles plus importantes et exploiter l'intelligence artificielle et d'autres outils pour fonctionner sans contrôle manuel. Par ailleurs, les drones ne fonctionnent pas seulement dans les airs. Le 3 mars 2020, comme j'en ai informé le Conseil, le groupe terroriste houthiste a utilisé un bateau-drone télécommandé chargé d'explosifs pour attaquer un pétrolier au large des côtes du Yémen. Si elle avait abouti, cette attaque aurait eu des effets dévastateurs, non seulement sur le pétrolier et son équipage, mais aussi sur l'environnement, sur les voies de ravitaillement mondiales et sur les communautés locales le long de la côte yéménite qui dépendent de la mer pour subsister. Nous sommes dans un contexte hobbesien en ce qui concerne l'utilisation de la technologie par des acteurs non étatiques surpuissants. L'inaction n'est pas une option, car en l'absence de réglementation, nous ne faisons qu'encourager la prolifération.

Aujourd'hui, il apparaît clairement, d'après les preuves présentées et d'autres informations dont nous disposons, que les groupes terroristes et les acteurs non étatiques ont de plus en plus accès à ces technologies. Nous condamnons avec force leur utilisation pour mener des attaques transfrontières et prendre pour cible des civils ou des infrastructures civiles, en violation du droit international. Mais cette menace ne fera que croître au fur et à mesure que la technologie progressera, et nous devons y faire face à l'ONU. Les gouvernements doivent renforcer la coordination, appuyer les mesures de renforcement des capacités et échanger des bonnes pratiques et des conseils pour contrer cette menace.

Enfin, nous avons parlé de l'importance des technologies numériques pour protéger les acteurs humanitaires. Parlons maintenant de leur rôle dans l'intensification de l'action humanitaire. Les innovations numériques telles que l'intelligence artificielle, l'analyse prédictive, les transferts numériques de fonds et la technologie de la chaîne de blocs peuvent améliorer les opérations humanitaires. Ces technologies émergentes aident non seulement les acteurs humanitaires à anticiper les crises et à s'y préparer, mais leur permettent également d'agir plus rapidement et plus efficacement lorsque ces crises surviennent.

Alors que nous examinons les questions liées à l'innovation numérique, n'oublions pas la fracture numérique. L'on estime que 37 % de la population mondiale, soit près de 3 milliards de personnes, n'a jamais utilisé Internet. Cette fracture reste importante, et elle touche les femmes et les filles de manière disproportionnée. Dans les pays les moins avancés, seules 19 % des femmes utilisent Internet, soit 12 % de moins que les hommes. Les inégalités dans le monde physique se transposent clairement dans le monde numérique. Alors que nous réfléchissons à la manière dont l'innovation peut nous aider à renforcer l'impact de notre action, donnons la priorité à celles et ceux qui n'ont pas encore récolté les dividendes des évolutions technologiques qui sont devenues banales dans d'autres régions du monde.

Les Émirats arabes unis, qui ont été parmi les premiers à défendre la technologie d'avant-garde, tirent parti de ses avantages au niveau national et international. C'est pourquoi, il y a quatre ans, nous avons mis tout notre poids derrière la création par le Secrétaire général du Groupe de haut niveau sur la coopération numérique, qui reflétait notre conviction que les technologies numériques peuvent contribuer concrètement à la paix et à la sécurité mondiales. Nous avons activement appuyé les activités de mise en œuvre et nous saluons l'idée d'établir un Pacte numérique mondial, proposée par le Secrétaire général dans son rapport intitulé *Notre Programme commun* (A/75/982). Nous devons tous continuer à défendre ces efforts multilatéraux.

Les Émirats arabes unis continueront à travailler avec toutes les personnes ici présentes et avec toutes les parties prenantes pour faire en sorte que le monde bénéficie des technologies numériques en tant qu'outil essentiel à l'avènement de sociétés plus résilientes, plus équitables et plus inclusives.

M. de Oliveira Marques (Brésil) (*parle en anglais*) : Le Brésil remercie la présidence des États-Unis d'avoir organisé la séance d'aujourd'hui sur les conséquences des technologies numériques sur le maintien de la paix et de la sécurité internationales. Nous remercions également de leurs exposés éclairants la Secrétaire générale adjointe aux affaires politiques et à la consolidation de la paix, M^me^ Rosemary DiCarlo, ainsi que M^me^ Nyabola et M. Druet.

Le processus de transformation numérique est source d'avantages et de possibilités considérables pour l'humanité, notamment pour consolider la paix et favoriser la compréhension et pour autonomiser les groupes sous-représentés et vulnérables.

La pandémie de maladie à coronavirus (COVID-19) a montré à la société les avantages considérables de l'utilisation des technologies numériques, qui se sont révélées des outils efficaces pour nous permettre de poursuivre nos activités quotidiennes, malgré les restrictions imposées par la menace du virus. Les systèmes éducatifs, commerciaux et bancaires, parmi beaucoup d'autres, ont pu adapter les technologies existantes à cette réalité nouvelle et imprévue. Le Conseil et le système des Nations Unies se sont servis de ces technologies pour continuer à organiser des réunions, et nous nous sommes désormais habitués à l'idée d'écouter des intervenants qui ne peuvent pas assister en personne à une réunion. Bien entendu, ces avantages n'ont pas été exploités de la même manière partout, en raison des inégalités persistantes dans l'accès aux technologies de l'information et de la communication. Combler cette fracture numérique demeure une tâche importante que doit accomplir la communauté internationale.

Comme nous le savons tous, les technologies numériques qui ont révolutionné nos vies en permettant la production, le stockage et la diffusion de grandes quantités d'informations, ainsi que l'accès à ces informations, sont souvent utilisées à mauvais escient par des gouvernements et des acteurs non étatiques. Le débat d'aujourd'hui a abordé certains de ces problèmes, qui sont par nature diversifiés et qui appellent donc des réponses différentes de la part des États.

L'Assemblée générale a reconnu que le droit international, en particulier la Charte des Nations Unies, s'applique aux activités menées par les États dans le cyberespace et qu'il est essentiel pour maintenir la paix et la stabilité, respecter les droits de l'homme et promouvoir un environnement numérique ouvert, sûr, pacifique et accessible. Le droit international des droits de l'homme et le droit international humanitaire doivent être respectés en ligne comme hors ligne. Nous soulignons également la nécessité d'adhérer aux normes volontaires et non contraignantes de comportement responsable des États dans le cyberespace approuvées par l'Assemblée générale, notamment en protégeant les infrastructures informatiques critiques qui soutiennent la fourniture de services essentiels au public.

Pour remédier au problème de la désinformation, les gouvernements et les sociétés doivent adopter des stratégies globales. Les campagnes d'éducation et les débats publics visant à sensibiliser le public, ainsi que la coopération entre les acteurs publics et privés tels que les médias sociaux, peuvent contribuer à lutter contre l'utilisation abusive des plateformes numériques à des fins d'incitation à la violence et au terrorisme.

La coopération internationale relative à l'utilisation des technologies numériques a considérablement renforcé notre capacité d'identifier les menaces communes, y compris celles provenant d'acteurs non étatiques tels que des groupes terroristes. Alors que les technologies évoluent, nous pouvons également les utiliser plus efficacement pour améliorer la transparence et l'agilité du Conseil de sécurité. Nous devons encourager l'utilisation des nouvelles technologies pour améliorer l'accès des femmes, des jeunes et de la société civile aux processus de paix et aux initiatives de consolidation et de maintien de la paix.

Les opérations de maintien de la paix des Nations Unies doivent utiliser le plein potentiel des technologies numériques existantes afin de renforcer la mise en œuvre de leurs mandats. Je tiens à souligner l'importance que revêtent les nouvelles technologies dans le contexte des communications stratégiques des missions de maintien de la paix. Les communications stratégiques jouent un rôle de facilitateur et ont un effet multiplicateur pour toutes les activités prescrites, notamment en ce qui concerne la protection des civils et les programmes pour les femmes et la paix et la sécurité. En outre, elles jouent un rôle crucial dans la lutte contre la mésinformation et la désinformation qui pourraient entraver l'exécution des mandats et menacer la sûreté et la sécurité des soldats de la paix.

M. Biang (Gabon) : Je vous remercie, Madame la Présidente, pour l'initiative de cette séance, qui nous donne l'occasion de nous pencher sur l'impact des technologies numériques dans le maintien de la paix et de la sécurité internationales. C'est en fait une question qui, ces derniers temps, prend de plus en plus de relief au sein du programme international pour la paix. Je voudrais remercier la Secrétaire générale adjointe Rosemary DiCarlo, ainsi que M^me^ Nyabola et M. Druet pour leurs exposés édifiants.

La thématique au cœur de nos échanges aujourd'hui nous rappelle, plus que jamais, que le progrès technologique a repoussé les limites de notre monde physique dans l'infini du numérique et du cybernétique.

Cela implique, d'une part, un élargissement de nos possibilités à tous les niveaux, y compris en matière de maintien de la paix et de la sécurité internationales, et d'autre part, une reconfiguration et un recalibrage des menaces à la paix et à la sécurité internationales.

Le maintien de la paix repose plus que jamais sur un solide écosystème de technologies et d'innovation qui vient non seulement renforcer les outils de gestion et de prévention des conflits, mais aussi favoriser une meilleure appréciation des situations, améliorer l'appui aux missions et faciliter une mise en œuvre plus robuste des mandats des opérations de maintien de la paix des Nations Unies, bien souvent dans des environnements complexes.

Le progrès technologique participe également au renforcement de la sécurité des soldats de la paix ainsi que des populations civiles et permet une amélioration des actions préventives, notamment dans le domaine humanitaire. L'utilisation des drones et des systèmes d'analyse de pointe est de plus en plus un recours de choix pour observer et anticiper les mouvements dans les zones difficilement accessibles, notamment les champs de bataille, afin de disposer d'informations fiables pour réagir opportunément et plus efficacement.

De façon manifeste, le monde est à un point de bascule vers une robotisation ou une numérisation de nos sociétés, de notre gouvernance aux échelles aussi bien nationale que mondiale et surtout de nos droits et de nos obligations. Cette mutation technologique n'a malheureusement pas que des avantages. Elle s'accompagne de conséquences et de sources de préoccupation, comme toute science qui n'est pas revêtue du manteau de la conscience.

Souvent considéré comme un multiplicateur de force, le progrès technologique se révèle également comme un facteur d'exacerbation des conflits mondiaux. En effet, les discours haineux, de radicalisation, d'incitation à la discrimination et à la violence sous toutes leurs formes, diffusés au moyen d'Internet et sur les réseaux sociaux, et dont les femmes et les jeunes sont les premières cibles vulnérables, sont devenus aujourd'hui des véhicules privilégiés de la terreur, de la peur et de la pérennisation des crises.

La fabrication d'armes plus puissantes et plus sophistiquées, affinées par les progrès technologiques, va avec une capacité de nuisance et de déshumanisation amplifiée qui doit être soumise à un encadrement juridique et déontologique strict au risque d'être un réel danger pour l'humanité. Le triste spectacle des bandes armées et groupes terroristes qui se dotent librement d'armes de plus en plus sophistiquées et de nouvelles technologies pour renforcer leur pouvoir de déstabilisation dans plusieurs régions en Afrique, nous interpelle sur la nécessité pour les soldats de la paix ainsi que les forces régulières des pays hôtes de disposer des technologies de pointe également.

Il en va de la viabilité des États en proie à ces forces négatives et de la survie des populations concernées, qui sont prises dans un terrible étau entre, d'un côté, l'impuissance des États à l'autorité décadente, et de l'autre côté, le supplice infligé par des bandes armées dont le programme de référence est la terreur et le chaos. Il est crucial que les forces de maintien de la paix puissent disposer d'équipements technologiques à la dimension de l'ampleur des nouvelles menaces et adaptés aux défis à relever, notamment dans les conflits armés asymétriques contre les groupes terroristes.

Nous partageons la conviction qu'il est nécessaire d'encourager l'innovation et le progrès technologiques sur le terrain ; de maximiser le potentiel des technologies actuelles et nouvelles en vue d'améliorer la capacité de nos missions de paix à s'acquitter efficacement de leurs mandats ; de permettre aux opérations de paix de détecter, d'analyser et de traiter les menaces contre les civils, les soldats de la paix et les missions humanitaires et politiques de manière opportune et intégrée ; et enfin de veiller à une utilisation plus responsable des technologies numériques par les opérations de paix, tout en respectant les droits de l'homme partout où il existe un risque de préjudice.

Mon pays soutient la Stratégie pour la transformation numérique du maintien de la paix des Nations Unies ainsi que la Stratégie et le Plan d'action des Nations Unies pour la lutte contre les discours de haine.

Le Gabon demeure résolument attaché à l'utilisation pacifique et responsable des technologies en faveur du maintien de la paix et de la sécurité internationales et appelle au renforcement de la coopération triangulaire qui est essentielle, entre autres, à la mise en œuvre de la résolution 2518 (2020) relative à la sûreté et à la sécurité des soldats de la paix.

Pour terminer, je voudrais souligner l'importance d'une mobilisation aux échelles internationale, régionale et nationale en vue de parvenir à une gouvernance optimale de l'espace numérique et du progrès technologique,

pour en faire de réels catalyseurs des mandats des missions de paix de l'ONU et des instruments d'envergure au service de la paix et de la sécurité internationales.

M^me^ Juul (Norvège) (*parle en anglais*) : Je tiens à remercier les intervenants de leurs déclarations très intéressantes. Je remercie également les États-Unis d'avoir facilité ce débat important au sein du Conseil de sécurité.

Au cours de l'année écoulée, le Conseil a tenu, sous différents formats, des débats sur la technologie et la sécurité, de la réunion sur les technologies émergentes et la sécurité organisée selon la formule Arria en mai 2021 par la Mission permanente de la Chine au débat public tenu en juin, lorsque l'Estonie a inscrit pour la première fois la cybersécurité à l'ordre du jour du Conseil (voir S/2021/621). La poursuite de cette discussion tombe à point nommé.

Les technologies numériques émergentes et en évolution présentent de grandes possibilités dans un certain nombre de domaines. En effet, sans les technologies numériques, le Conseil de sécurité lui-même n'aurait pas été en mesure de poursuivre ses travaux durant les premiers temps de la pandémie de maladie à coronavirus (COVID-19). Dans le même temps, les technologies numériques peuvent aussi susciter des préoccupations et des problèmes. Lorsqu'elles sont utilisées à des fins malveillantes, elles représentent incontestablement une menace pour la paix et la sécurité internationales. La discussion d'aujourd'hui est donc au cœur du mandat et de la responsabilité du Conseil.

Il n'y a pas que les États qui mobilisent et utilisent les technologies numériques. Cela souligne l'importance de la coopération entre les États et les autres parties prenantes. Nous devons coopérer avec tous ceux qui mettent au point et utilisent les technologies, y compris les milieux universitaires et les organisations non gouvernementales. Ce n'est qu'en travaillant ensemble que nous pouvons veiller à ce que les nouvelles technologies nous aident à aller de l'avant dans un sens qui nous profite à tous. L'ONU constitue une importante plateforme mondiale pour une telle interaction.

Le détournement des technologies numériques peut nuire à la paix et à la sécurité à l'échelle mondiale, par exemple en cas de panne d'Internet ou de propagation rapide de fausses informations. La Norvège s'inquiète que l'évolution du détournement du domaine numérique puisse entraîner une montée des tensions, y compris des violations des droits de l'homme et des atteintes à ces droits. Les restrictions délibérées de l'accès à Internet, totales ou partielles, ne représentent qu'un type de détournement parmi d'autres. La diffusion de fausses informations ciblées par l'intermédiaire des technologies numériques en est un autre, qui limite souvent l'accès des gens à des informations fiables quand ils en ont le plus besoin.

Néanmoins, nous ne devons pas sous-estimer les effets positifs des technologies numériques. Elles peuvent aider à promouvoir l'inclusion dans les processus de décision en y donnant accès à des groupes traditionnellement exclus, tels que les femmes et les minorités, y compris au moyen de visioconférences au Conseil de sécurité lui-même pour faciliter la participation d'intervenants de la société civile plus nombreux et variés.

La désinformation reste aussi un problème dans de nombreux domaines, notamment dans la mesure où elle fait peser un risque sur nos propres missions de maintien de la paix des Nations Unies, par exemple, quand de fausses informations sont propagées pour créer un climat plus hostile dans les communautés que les soldats de la paix sont censés aider. La meilleure défense contre la désinformation réside dans un secteur médiatique libre, indépendant et professionnel. Il est essentiel que les médias soient libres de communiquer des informations importantes, de poser des questions critiques et de rendre compte des violations des droits humains et des atteintes à ces droits. L'appui à des médias indépendants et pluralistes et d'assurer la sécurité des journalistes peut donc aider à réduire les tensions et à prévenir les conflits.

Je vous remercie une fois encore, Madame la Présidente, d'avoir inscrit cette question à notre ordre du jour. J'espère bien que ce sera une discussion qui se poursuivra sur la manière dont nous pouvons éviter et contrer la désinformation et d'autres problèmes dus au détournement des technologies numériques, sans perdre de vue les immenses avantages que ces technologies apportent au maintien de la paix et de la sécurité internationales.

M. Roscoe (Royaume-Uni) (*parle en anglais*) : Je vous remercie, Madame la Présidente, pour la discussion de ce jour. Nous sommes également très reconnaissants aux intervenants de leurs contributions, qui ont montré que la technologie changeait la manière dont nous surveillons, comprenons et affrontons les conflits et les crises humanitaires dans le monde.

Premièrement, il est clair que la technologie peut jouer un rôle dans la prévention effective des conflits. Si nous pouvons anticiper les risques, nous pouvons et devons agir avant qu'une crise n'éclate. Des décisions prises au moment opportun permettent de mener des interventions rapides et préventives, un domaine, que, à mon avis, le Conseil de sécurité devrait explorer de plus près, en liaison avec le Secrétariat. C'est aussi pourquoi nous travaillons avec d'autres et l'industrie pour élaborer des modèles de prévention des conflits axés sur l'intelligence artificielle.

Deuxièmement, durant les conflits eux-mêmes, il est essentiel que les Casques bleus en mission aient une perception exacte de la situation. La combinaison de technologies numériques, comme la surveillance à distance avec de meilleurs processus de renseignement, de surveillance et de reconnaissance, peut permettre aux missions de maintien de la paix et de surveillance d'améliorer leur compréhension des menaces et des vulnérabilités sur le terrain. Si nous pouvons obtenir que les drones décrits par notre collègue des Émirats arabes unis aident les soldats de la paix au lieu d'attaquer des gens, nous pouvons progresser.

Troisièmement, la technologie permet également une meilleure attribution des responsabilités. Comme nous l'avons entendu aujourd'hui, notamment de nos brillants intervenants, les médias sociaux offrent la possibilité de mieux identifier les coupables ; ils donnent aux gens les moyens d'informer le monde sur les conflits, comme ils les vivent, de telle sorte que le monde sache ce qui se passe d'après les personnes qui sont aux premières loges. Cela veut dire que la vérité, y compris les preuves d'atrocités de masse ou de violations généralisées du droit international humanitaire, ne peut pas être cachée par ceux qui voudraient la cacher.

Nous l'avons aussi entendu aujourd'hui, la technologie est utilisée par des États et d'autres acteurs afin de priver les individus de leurs droits humains et de propager de fausses informations comme outils des conflits. Nous constatons que certains États tentent de cacher la vérité en bloquant l'accès aux médias sociaux ou aux sites de médias indépendants. Comme d'autres l'ont noté, nous avons vu cela l'an dernier quand la junte militaire a coupé Internet au Myanmar. Nous voyons également des régimes autoritaires utiliser la technologie de surveillance pour suivre et persécuter leurs propres citoyens, en leur refusant l'exercice de leurs droits fondamentaux. La technologie peut aussi être employée par ceux qui cherchent à déstabiliser, et c'est particulièrement vrai dans le contexte de l'invasion russe de l'Ukraine, où la Russie mène des cyberattaques et, nous l'avons signalé, se sert d'une usine de trolls en ligne pour diffuser de fausses informations et manipuler l'opinion publique au sujet de sa guerre illégale.

Heureusement, la technologie peut également aider à combattre la désinformation. La Russie a prétendu une fois de plus aujourd'hui que les dépouilles de victimes étalées dans les rues de Boutcha étaient une « provocation montée de toutes pièces » par l'Ukraine. Elle a suggéré que les forces ukrainiennes avaient mis en scène cette provocation après avoir repris la ville. Toutefois, l'imagerie satellite a prouvé que les cadavres dans les rues de Boutcha étaient là depuis plusieurs semaines, ce qui établit clairement que les personnes tuées l'ont été durant la période où les forces russes occupaient la ville.

Aujourd'hui, au lieu d'un discours sur une provocation montée de toutes pièces, on nous a servi de nouvelles absurdités sur une artillerie obsolète. Il s'agit d'une nouvelle tactique russe pour tenter de nous distraire, de nous tromper et de nous enfumer – des couches de mensonges contradictoires et concurrents afin de créer la confusion chez les gens au point qu'ils ne sachent plus quoi croire. Cependant, nul ne doit se laisser berner. Nous attendons avec intérêt que la Cour pénale internationale ouvre une enquête en bonne et due forme pour que nous puissions savoir la vérité sur ce qui s'est produit à Boutcha, sur la base de preuves concluantes. On peut espérer qu'il en découlera des inculpations.

La lutte contre la mésinformation et la défense des médias déterminés à exposer la vérité en ligne sont cruciales pour le bon fonctionnement du système international. Par conséquent, lorsque la délégation russe se plaint d'être sanctionnée sur les médias sociaux ou que ses organes de propagande d'État soient bloqués, elle ne devrait pas. Dans l'espace numérique, comme dans tous les espaces, nous devons nous efforcer de protéger la vérité de ce nouveau double langage.

Il nous faut travailler ensemble, y compris avec les organisations de la société civile, le secteur privé et d'autres communautés, pour bien comprendre les avantages des technologies numériques et contrer les risques qu'elles recèlent. Cela supposera d'adapter les institutions et de défendre les règles qui sont ancrées dans des normes strictes, dans les droits humains et dans les valeurs démocratiques. Le Conseil doit veiller dans le même temps à ce que les cadres en place et le droit

international restent nos principes directeurs. Si nous réussissons, nous pourrons garantir que les technologies numériques soient une force du bien et l'occasion d'une transformation pour la pérennisation de la paix et du développement.

M. Flynn (Irlande) (*parle en anglais*) : Je remercie nos intervenants.

Comme nous l'avons entendu aujourd'hui, la technologie est une force positive au service du bien dans notre vie mais peut également être une arme puissante pour fomenter la violence et les conflits. Les cyberattaques, la cybercriminalité et le détournement de la technologie pour propager la désinformation portent gravement atteinte à la confiance, tandis que les avancées de la technologie moderne contribuent à modifier la nature des conflits. Les discours de haine peuvent être diffusés et amplifiés en quelques minutes, polarisant ainsi des communautés, sapant la démocratie et attisant l'intolérance et la violence dans le monde entier.

Les exemples de ces risques sont innombrables. Les médias russes contrôlés par l'État ont mené une campagne de désinformation dans le but de créer un prétexte à la guerre illégale de la Russie en Ukraine. La guerre se poursuit, tout comme les efforts déployés par la Fédération de Russie pour déformer la réalité et nier son agression brutale sur le terrain.

Au Myanmar, comme d'autres orateurs l'ont dit, les restrictions à l'accès à Internet avant le coup d'État étaient un signe précurseur de l'érosion des libertés fondamentales, de la répression, de la surveillance et de la violence brutale qui ont suivi. En Éthiopie, nous avons été témoins de l'utilisation abusive des technologies pour opprimer les défenseurs des droits de l'homme, surveiller les militants, diffuser des discours de haine et provoquer des tensions par l'entremise des médias sociaux. Dans plusieurs autres cas, les nouvelles technologies sont utilisées à mauvais escient pour porter atteinte à la sécurité et à l'intégrité des États, attaquer les infrastructures critiques, interférer dans les processus démocratiques et restreindre les droits humains.

La prolifération des technologies numériques présente de nouveaux risques et défis, mais elle peut également jouer un rôle important à l'appui de la paix. De la Colombie à la Libye, nous avons vu comment les technologies numériques ont été utilisées pour promouvoir l'inclusion, encourager la participation aux processus de paix et compléter les échanges en personne. Elles peuvent et doivent faciliter et renforcer la participation des femmes, des jeunes et des minorités. L'Irlande salue le travail effectué par le Groupe de l'appui à la médiation et de la Cellule Innovation du Département des affaires politiques et de la consolidation de la paix à cet égard. Toutefois, ces efforts doivent tenir compte des risques spécifiques auxquels ces groupes sont confrontés dans les espaces en ligne et de la fracture numérique entre les sexes dans le monde.

Nous encourageons toutes les personnes qui sont autour de cette table à être plus disposées à examiner l'incidence positive que la technologie peut avoir s'agissant de prévenir les conflits et de relever les défis internationaux tels que les changements climatiques. Les mesures et initiatives de renforcement des capacités et de confiance, y compris le programme d'action pour favoriser le comportement responsable des États dans le cyberespace, que l'Irlande a été fière de coparrainer, sont au centre de ces efforts.

La technologie peut également agir comme un multiplicateur de force dans les missions de maintien de la paix, en permettant aux soldats de la paix de mieux appréhender les diverses situations et en leur offrant de meilleures capacités d'analyse des données. Ces outils d'une importance cruciale permettent d'améliorer la sûreté, la sécurité et l'efficacité des opérations, facilitant ainsi l'exécution des mandats. C'est pourquoi la mise en œuvre de la Stratégie pour la transformation numérique du maintien de la paix des Nations Unies est si importante.

C'est précisément en période de conflit armé que nous devons défendre fermement le droit à la liberté d'expression, en ligne comme hors-ligne, et l'accès à l'information. En effet, ces libertés sont essentielles pour promouvoir une paix durable, comprendre la nature des conflits et garantir l'application du principe de responsabilité. Aujourd'hui, je rends hommage aux citoyens, aux journalistes et aux défenseurs des droits humains en Ukraine qui utilisent les technologies numériques pour partager des histoires poignantes depuis les lignes de front, souvent au prix de grands risques personnels. Ils travaillent sans relâche pour recueillir, vérifier et préserver les preuves numériques des attaques, dans l'espoir qu'elles seront utilisées pour demander des comptes aux responsables.

Il ne fait aucun doute que le droit international, notamment le droit international humanitaire et le droit international des droits de l'homme, s'applique dans le

cyberespace. Nos approches relatives aux technologies numériques doivent être fondées sur les droits de l'homme, l'état de droit et les valeurs démocratiques.

L'Irlande appuie un cyberespace libre, sûr, sécurisé, inclusif et accessible. Nous savons que les technologies numériques n'existent pas dans le vide. Il est clair que les acteurs non étatiques jouent un rôle de premier plan en matière d'innovation technique. Il est essentiel que la société civile, notamment les défenseurs des droits humains, les groupes de femmes, les experts techniques, le monde universitaire et le secteur privé, participe activement et réellement à nos efforts pour trouver des solutions aux défis communs. En outre, l'Irlande encourage vivement la Commission de consolidation de la paix à tenir compte de l'incidence des technologies numériques, tant positive que négative, dans ses débats et les conseils qu'elle donne.

Pour conclure, investir dans le potentiel des technologies numériques, c'est investir dans la paix. S'agissant de l'utilisation des technologies numériques, l'Irlande est fermement convaincue que le multilatéralisme, le comportement responsable des États, la transparence et la responsabilité humaine sont nécessaires pour renforcer et maintenir la confiance qui sous-tend la paix et la sécurité internationales.

La Présidente (*parle en anglais*) : Je vais maintenant faire une autre déclaration en ma qualité de représentante des États-Unis.

Pour commencer, je remercie tous mes collègues d'avoir pris part aujourd'hui à un dialogue très constructif sur le rôle que jouent les technologies numériques dans la promotion de la paix et de la sécurité internationales. Malheureusement, la Russie a choisi de ne pas être constructive en lançant des attaques sans fondement pour répandre délibérément le type de désinformation, qui est, en partie, la raison pour laquelle nous sommes réunis ici aujourd'hui, pour examiner les moyens de la prévenir et de la contrer.

Je ne vais pas m'attarder sur les théories délirantes du complot de la Russie. Au lieu de cela, en collaboration avec tous les autres membres du Conseil, nous allons poursuivre ces conversations importantes dans les semaines et les mois à venir. Je remercie une fois de plus les intervenants de leurs contributions aujourd'hui. Je remercie également tous mes collègues.

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

La séance est levée à 12 h 35.