Nations Unies A/C.1/77/PV.19

Assemblée générale

Soixante-dix-septième session

Documents officiels

Première Commission

19e séance plénière

Lundi 24 octobre 2022, à 15 heures

New York

Président : M. Pieris . . . . . (Sri Lanka)

La séance est ouverte à 15 h 5.

Points 90 à 108 de l'ordre du jour (*suite*)

Examen thématique des questions à l'ordre du jour et présentation et examen de tous les projets de résolution et de décision déposés au titre de tous les points de l'ordre du jour relatifs au désarmement et à la sécurité internationale

Le Président (*parle en anglais*) : La Première Commission va maintenant poursuivre le débat thématique sur le groupe de questions « Autres mesures de désarmement et sécurité internationale ». Les délégations qui souhaitent exercer leur droit de réponse pourront le faire une fois que la Commission aura entendu tous les orateurs et oratrices inscrits sur la liste pour ce groupe de questions. Si le temps le permet, la Commission entamera cet après-midi l'examen du groupe de questions « Désarmement et sécurité sur le plan régional ».

Avant de donner la parole aux délégations, je leur rappelle que, dans le cadre du débat thématique, la durée des déclarations est de cinq minutes lorsqu'elles s'expriment au nom de leur pays et de sept minutes lorsqu'elles le font au nom de plusieurs délégations.

M. Lagardien (Afrique du Sud) (*parle en anglais*) : L'Afrique du Sud s'associe à la déclaration faite par la représentante de l'Indonésie au nom du Mouvement des pays non alignés (voir A/C.1/77/PV.18).

L'Afrique du Sud a souscrit aux conclusions de 2021 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 premier groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation. Il est néanmoins important de rester unis derrière un processus unique, et nous attendons avec intérêt les travaux des quatrième et cinquième sessions du deuxième groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation. À cet égard, nous félicitons les États Membres d'avoir adopté par consensus le rapport d'activité annuel de 2022 du groupe de travail à composition non limitée (voir A/77/275), et nous espérons bien qu'un accord sera trouvé sur la sécurité numérique.

L'Afrique du Sud reste préoccupée par la menace croissante des cyberattaques contre les infrastructures critiques et les infrastructures d'information. Nous estimons qu'il faut répondre à ces menaces en coopérant davantage et en créant des mécanismes consacrés aux meilleures pratiques, tout en rappelant que ces efforts doivent être faits à l'appui des priorités nationales et de l'action menée pour identifier et définir lesdites infrastructures. Les États, en particulier les pays en développement, ne sont pas exposés au même niveau de risque, puisque tous n'ont pas les mêmes moyens de se prémunir contre des actes de malveillance dans le cyberespace. Dans ce contexte, l'Afrique du Sud insiste sur l'importance de l'application et du développement

des normes existantes. Ma délégation donne la priorité à la mise en œuvre qui, selon nous, contribuera à une meilleure compréhension des éventuelles lacunes des normes existantes, ce qui nous permettra alors d'évaluer la nécessité d'élaborer de nouvelles normes. La mise en œuvre est également l'occasion d'identifier les pratiques efficaces et les besoins en matière de renforcement des capacités.

L'Afrique du Sud se félicite des efforts déployés afin d'élaborer un programme d'action dans le cadre des travaux du groupe de travail. Nous sommes convaincus que les discussions qui seront menées au sein du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation nous permettront de mieux comprendre les menaces et les vulnérabilités des États qu'il conviendra d'inclure à ce programme d'action. L'Afrique du Sud, qui soutient depuis longtemps l'élaboration d'un tel programme d'action, reste d'avis que le groupe de travail à composition non limitée est l'organe approprié pour mener ce projet à bien. Nous rappelons à ce titre la recommandation figurant dans le rapport d'activité annuel du groupe de travail, selon laquelle ce dernier doit poursuivre l'élaboration du programme d'action, afin qu'il serve éventuellement de mécanisme destiné à promouvoir un comportement responsable des États dans l'utilisation des technologies de l'information et des communications (TIC), qui soutiendrait, entre autres, leur capacité à mettre en œuvre les engagements pris au titre de l'utilisation des TIC.

Nous pensons également que la participation active de tous les acteurs concernés, y compris la société civile et le secteur privé, est susceptible d'enrichir le processus mené par les États Membres, notamment pour mieux comprendre la nature des menaces, coopérer davantage et faire face de manière adéquate aux menaces posées par les acteurs étatiques et non étatiques à tous les niveaux de la société.

M. Röethlin (Autriche) (*parle en anglais*) : L'Autriche s'associe à la déclaration qui a été faite au nom de l'Union européenne (voir A/C.1/77/PV.18). À titre national, nous voudrions formuler les observations suivantes.

Depuis le précédent débat consacré à ce groupe de questions, en 2019, l'importance de la cybersécurité s'est considérablement accrue. Malheureusement, nous avons également dû constater les dommages considérables que peuvent engendrer les comportements irresponsables et illégaux dans le cyberespace. Avec leurs répercussions non seulement sur l'Ukraine, mais aussi sur d'autres pays, les cyberattaques illégales qui accompagnent l'invasion de l'Ukraine par la Russie en sont un bon exemple.

Nous nous félicitons donc de l'attention accrue accordée par l'Organisation des Nations Unies à la cybersécurité, et saluons le travail important réalisé par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, qui a achevé avec succès sa première année de travail en adoptant un rapport d'activité (voir A/77/275), que la Commission accueillera, nous l'espérons, favorablement par consensus. Le rapport et ses recommandations jettent les bases des futurs travaux du groupe. Nous nous félicitons aussi de la participation active de diverses parties prenantes, même si nous regrettons qu'un grand nombre d'acteurs importants de l'industrie, du monde universitaire et de la société civile aient été empêchés de participer à ses travaux en raison de veto dénués de fondements. Nous ne pouvons pas agir sur la cybersécurité sans échanges avec les principales parties prenantes qui la façonnent.

L'Autriche continuera dès lors de plaider en faveur d'un cyberespace ouvert, libre, stable et sûr, fondé sur la pleine applicabilité du droit international, y compris le droit international humanitaire et le droit international des droits de l'homme, et guidé par le cadre favorisant un comportement responsable des États dans le cyberespace, adopté par consensus.

Beaucoup reste à faire, notamment en ce qui concerne la portée exacte de l'applicabilité du droit international et des mesures de confiance et de renforcement des capacités. Nous poursuivrons nos efforts en ce sens au sein du groupe de travail et espérons que les bonnes pratiques existantes dans ces domaines pourront notamment être examinées, notamment en incluant des échanges avec des organisations régionales dans le cadre du groupe de travail. Nous sommes convaincus qu'un programme d'action peut être un vecteur idéal pour progresser dans la mise en œuvre du cadre normatif, c'est pourquoi nous soutenons le projet de résolution (A/C.1/77/L.73) sur le programme d'action, déposé par la France.

Le fait que les projets de résolution portant sur ce groupe de questions couvrent des aspects importants de l'action menée dans le domaine du désarmement et de la sécurité internationale, des aspects qui ont été trop longtemps négligés, est très encourageant. Je souhaite à ce titre aborder brièvement deux points.

Tout d'abord, nous saluons l'action importante et soutenue menée ces dernières années par le Bureau des affaires de désarmement dans le domaine de l'éducation au désarmement. En ces temps de tensions accrues à l'échelle mondiale, il est de plus en plus important de bien communiquer sur notre travail. Cela permettra de

sensibiliser l'opinion publique et nous aidera à former les prochaines générations d'experts qui effectuent un travail essentiel dans le domaine du désarmement.

Deuxièmement, ces dernières années, le monde a été confronté non seulement à des conflits armés, mais aussi à une pandémie mondiale et aux conséquences de plus en plus graves des changements climatiques. Pourtant, l'allocation des ressources entre ces trois pôles de crise n'a pas été égale. Nous voudrions à ce titre réitérer notre appel de l'année dernière en réaffirmant qu'à nos yeux, croire que la sécurité ne peut être assurée que par l'armement militaire est une illusion dangereuse. Les crises non militaires dont nous sommes témoins doivent nous inciter à élargir notre conception de la sécurité et à mieux intégrer les instruments et les mesures de désarmement dans tous les efforts que nous déployons pour instaurer et maintenir la sécurité.

M. De Martin Topranin (Italie) (*parle en anglais*) : L'Italie s'associe à la déclaration prononcée au nom de l'Union européenne (voir A/C.1/77/PV.18) et voudrait faire les observations supplémentaires suivantes à titre national.

Le développement technologique et le progrès scientifique sont essentiels au bien-être de l'humanité et doivent être considérés comme un instrument de promotion de la paix et de la croissance durable. Les technologies de l'information et des communications (TIC) et Internet comptent parmi les plus grandes réalisations humaines de tous les temps et offrent des possibilités sans précédent. Au cours de nos travaux sur le désarmement et la sécurité, nous avons l'importante responsabilité de veiller à ce que ces évolutions s'opèrent dans un cadre approprié et d'empêcher leur utilisation dangereuse ou malveillante.

La coopération internationale est essentielle pour atteindre cet objectif. Aussi devons-nous améliorer le dialogue, la transparence et les mesures de confiance afin de promouvoir une meilleure compréhension des défis auxquels nous sommes toutes et tous confrontés. L'Italie reste attachée au concept de cyberstabilité, qui soutient les efforts déployés par la communauté internationale en faveur d'un cyberespace fondé sur l'applicabilité et le respect du droit international dans son intégralité, à commencer par la Charte des Nations Unies, le droit international humanitaire et le droit international des droits de l'homme.

Nous soutenons dès lors pleinement les travaux en cours du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation et nous nous félicitons du succès de sa troisième session de fond, ponctuée par l'adoption par consensus d'un rapport d'activité annuel. Nous soutenons donc sans réserve le projet de décision présenté par Singapour au nom du Président afin que ce rapport (voir A/77/275) soit adopté par consensus. En tant que fervents défenseurs du multilatéralisme et de méthodes de travail associant toutes les parties prenantes et s'appuyant sur les acquis, nous pensons qu'il faut e exploiter tout le potentiel des discussions à venir sur cette question. Le dialogue institutionnel doit être ordonné, prévisible et ouvert à toutes les parties prenantes afin de permettre des progrès constructifs, rapides et financièrement rentables.

Il importe de reconnaître que l'intensification et l'évolution des TIC s'accompagnent d'une augmentation des menaces. Il s'agit là d'un autre sujet important sur lequel le groupe de travail devrait intensifier ses travaux, en particulier en ce qui concerne la cyberrésilience des infrastructures numériques et les menaces posées par l'utilisation de la cybernétique dans les conflits armés. Ces questions sont particulièrement pressantes dans le contexte géopolitique actuel et après la guerre d'agression non provoquée et injustifiée de la Russie contre l'Ukraine.

Cet acte brutal a permis de mettre en évidence la dépendance des activités critiques des sociétés connectées à l'égard de l'infrastructure numérique, en particulier l'infrastructure de télécommunications, et les vulnérabilités qui en découlent. L'Italie souligne à cet égard l'importance de protéger les infrastructures numériques contre les ingérences malveillantes et appelle tous les acteurs à soutenir en priorité la résilience des infrastructures d'information, de communication et de télécommunication. Cet aspect est essentiel pour garantir l'accès aux réseaux Internet mondiaux qui sous-tendent l'accès à l'information, y compris les informations vitales et les entreprises.

Nous avons la ferme volonté d'accroître la cyber-résilience des infrastructures numériques, d'améliorer le niveau des connaissances en matière de cybermenaces et de développer une cyberréaction coordonnée, conformément à nos cadres de cybersécurité et de sécurité nationale et aux initiatives de coopération et de partenariat existantes et futures.

Nous savons désormais que le domaine cybernétique est un contexte très dynamique, et nous pensons qu'il est nécessaire de renforcer notre action pour que nos débats se traduisent en progrès tangibles qui améliorent la coopération internationale en matière de cybersécurité. Dans cet esprit, l'Italie soutient la proposition de

créer un programme d'action destiné à promouvoir le comportement responsable dans le cyberespace en tant qu'initiative nécessaire pour un programme orienté vers l'action (A/C.1/77/L.73). Ce doit être un processus ouvert à tous, mené sous l'égide des États Membres de l'ONU. Nous pensons qu'en cette période délicate, nous devons unir nos forces et conférer une dimension opérationnelle à notre dialogue institutionnel.

Nous soutenons donc pleinement le programme d'action sur le cyberespace, que nous voyons comme un projet extrêmement censé, inclusif et équilibré, capable d'ouvrir un dialogue opérationnel axé sur la mise en œuvre, tout en s'appuyant sur nos acquis. Sur le plan des actions, qu'il me soit permis de souligner que le renforcement des capacités est essentiel à la mise en place et au maintien d'un cyberespace sûr et sécurisé.

M. Shin (Fédération de Russie) (*parle en russe*) : Pour commencer ma déclaration, je souhaite souligner une fois encore que la Fédération de Russie promeut en toutes circonstances un programme unificateur dans le domaine de la maîtrise des armements, du désarmement et de la non-prolifération. Nous avons déposé le projet de résolution A/C.1/77/L.66, intitulé « Renforcement et développement du système de traités et d'accords sur la maîtrise des armements, le désarmement et la non-prolifération ». Nous espérons qu'il sera adopté par consensus et qu'il aura un effet positif sur la coopération, que nous espérons constructive, sur l'ensemble des questions relatives à la paix et à la sécurité internationales.

S'agissant du point 94 de l'ordre du jour, le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) a été créé en 2020 à l'initiative de la Fédération de Russie et avec le soutien massif des États Membres de l'Organisation des Nations Unies. Ce groupe de travail est le seul mécanisme de négociation sur ces questions au sein du système des Nations Unies. Ce format a l'avantage de permettre à tous les États, sans exception, de participer directement au processus de prise de décision sur les questions qui ont une incidence sur la sécurité nationale et de discuter de toutes les initiatives pertinentes des États sur une base véritablement démocratique, ouverte et transparente.

Dans ce contexte, nous nous félicitons des avis exprimés en appui au groupe de travail par la représentante de l'Indonésie au nom du Mouvement des pays non alignés, le représentant des Philippines au nom de l'Association des nations de l'Asie du Sud-Est, le représentant du Belize au nom de la Communauté des Caraïbes, et le représentant de l'Iraq au nom du Groupe des États arabes (voir A/C.1/77/PV.18), ainsi que de la volonté de ces entités de poursuivre un travail constructif dans le cadre de ce format.

La première année des travaux du groupe de travail s'est achevée par l'adoption par consensus, le 29 juillet, de son rapport d'activité annuel (voir A/77/275), qui contient des dispositions importantes permettant de créer une base pour l'élaboration d'un régime juridique international visant à réglementer l'utilisation des technologies de l'information et des communications (TIC) et à développer la coopération interétatique dans ce domaine. La Fédération de Russie estime qu'il est essentiel non seulement de consolider les succès déjà obtenus, mais aussi d'inciter le groupe de travail à mener d'autres négociations constructives afin de convenir de mesures spécifiques pour renforcer la paix et la sécurité dans la sphère de l'information et d'aborder les questions relatives au développement numérique.

À cette fin, la Russie a déposé le projet de résolution A/C.1/77/L.23/Rev.1, intitulé « Progrès de l'informatique et des télécommunications et sécurité internationale », dont des versions antérieures ont été déposées chaque année par la Russie depuis 1998. Le projet de résolution A/C.1/77/L.23/Rev.1 est universel, non conflictuel et non politisé. Il complète le projet de décision A/C.1/77/L.54, déposé par Singapour, qui approuve le rapport d'activité annuel du groupe de travail, et salue les efforts déployés par la présidence du groupe, que nous soutenons pleinement. Le projet de résolution A/C.1/77/L.23/Rev.1 est basé sur les dispositions des résolutions précédemment adoptées par l'Assemblée générale, ainsi que sur les rapports de consensus du premier et de l'actuel groupe de travail. L'objectif est de préserver le groupe en tant que plateforme de négociation clef traitant de l'ensemble des questions de sécurité internationale de l'information sous les auspices de l'ONU et d'empêcher sa fragmentation en formats parallèles qui font double emploi. Telle est l'aspiration de la communauté internationale dans son ensemble, et que le groupe incarne.

Le projet de résolution A/C.1/77/L.23/Rev.1 confirme l'accord conclu précédemment par consensus visant à développer davantage toutes les initiatives nationales sur la sécurité dans l'utilisation des TIC au sein du groupe de travail. Il contient des propositions spécifiques sur le renforcement des capacités dans l'utilisation des TIC et confirme également la nécessité de décider du format futur du dialogue institutionnel régulier sur ces questions sur une base véritablement universelle, au sein du groupe existant. En outre, un tel mécanisme ne devrait être mis

en place qu'à l'issue des travaux du groupe de travail en 2025. Nous devons donner au groupe une chance de réaliser pleinement son potentiel au cours des trois années restantes de son mandat.

L'adoption du projet de résolution A/C.1/77/L.23/Rev.1, déposé par la Russie, est particulièrement importante cette année dans la mesure où un groupe d'États a déposé un projet de résolution (A/C.1/77/L.23) qui propose essentiellement de créer un format qui remplacerait celui du groupe de travail à composition non limitée. Nous considérons qu'il s'agit là d'une nouvelle tentative de détourner les activités du groupe afin de politiser les négociations et d'imposer à la communauté internationale une décision prématurée quant à la forme que prendront les futurs travaux dans ce domaine. Nous trouvons cette approche inacceptable. Elle va à l'encontre de la logique et des intérêts de l'immense majorité des pays. Nous appelons les États Membres de l'Organisation des Nations Unies à soutenir le projet de résolution A/C.1/77/L.23/Rev.1, qui vise à préserver et à protéger le format actuel du groupe de travail à composition non limitée. Un vote pour le projet de résolution A/C.1/77/L.23/Rev.1 n'est pas un vote en faveur de la Russie, c'est un vote en faveur de la poursuite d'une action interétatique constructive et de négociations axées sur les résultats dans l'intérêt du renforcement de la paix, de la sécurité et de la stabilité dans la sphère de l'information.

M. Aidid (Malaisie) (*parle en anglais*) : La Malaisie s'associe aux déclarations faites par la représentante de l'Indonésie au nom du Mouvement des pays non alignés et par le représentant des Philippines au nom de l'Association des nations de l'Asie du Sud-Est (voir A/C.1/77/PV.18).

L'évolution rapide des technologies de l'information et des communications (TIC) a incontestablement créé des possibilités inestimables pour les peuples du monde entier, en favorisant la croissance socioéconomique et l'interaction transfrontalière dans divers domaines. Les outils numériques ont joué un rôle clef en facilitant le fonctionnement continu des entités publiques et privées aux niveaux national, régional et international pendant toute la durée de la pandémie de maladie à coronavirus (COVID-19), atténuant ainsi les coûts immenses de cette crise mondiale sans précédent. La dépendance qui est la nôtre aujourd'hui à l'égard des TIC, sans équivalent dans l'histoire de l'humanité, nous rappelle brutalement la nature des défis qui en découlent et l'importance d'une action collective pour les relever. Alors que nous tentons de faire face aux multiples répercussions de la pandémie de COVID-19, nous devons veiller à l'utilisation optimale de nos ressources limitées dans le domaine de la sécurité des technologies de l'information et des communications. Une attention particulière doit être accordée dans ce cadre aux besoins des pays en développement, tant pour ce qui est de l'application des règles, normes et principes existants qu'en ce qui concerne le discours mondial sur la poursuite de leur développement.

La complexité et la sophistication croissantes des menaces émergentes dans le cyberespace ont de quoi préoccuper. Nous devons rester vigilants face à toute utilisation malveillante des TIC, en particulier contre les infrastructures et les services essentiels. La poursuite du dialogue et de l'action par l'entremise de plates-formes multilatérales est essentielle si nous voulons combler les écarts de développement et tirer pleinement parti des TIC. À cet égard, la Malaisie souligne le rôle central du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et se félicite de l'adoption de son rapport d'activité annuel pour 2022 (voir A/77/275). En tant que plateforme universelle, ce groupe de travail offre un espace à tous les États Membres, notamment pour poursuivre l'élaboration des règles, normes et principes de comportement responsable des États, ainsi que leurs moyens de mise en œuvre. Le groupe de travail à composition non limitée offre également aux États Membres un moyen de s'engager durablement avec les parties prenantes qui font partie intégrante du développement, du fonctionnement et de la sécurité des outils numériques.

L'année dernière, notre pays a eu le plaisir de se porter coauteur de la résolution 76/19, qui souligne notamment le soutien des États Membres à l'actuel groupe de travail à composition non limitée et à son mandat. L'adoption sans vote de cette résolution a été une évolution positive, signifiant la volonté commune des États Membres de l'Organisation des Nations Unies de traiter les questions relatives aux TIC dans le cadre d'une plateforme unique, après plusieurs années de débats houleux sur différents mécanismes. À la présente session de la Première Commission, nous avons malheureusement vu des recommandations formulées par diverses délégations quant à l'intention sous-jacente et le bien-fondé des propositions avancées par d'autres. Il s'agit là d'un schéma récurrent que nous ne connaissons hélas que trop bien. La Malaisie espère vivement que les parties concernées mettront tout en œuvre pour coopérer de manière constructive et empêcher l'effritement d'un consensus durement acquis, qui, bien que fragile, a contribué à faire avancer les travaux du groupe de travail

à composition non limitée. Il est évident que toutes les parties reconnaissent la valeur du groupe de travail et l'impératif de préserver son intégrité et sa crédibilité. Comme beaucoup d'autres, la Malaisie est convaincue que ce groupe est l'organe le mieux à même de relever les défis qui se posent dans le domaine de la sécurité des TIC. Nous continuerons à participer activement aux réunions du groupe, qui constitue lui-même une mesure de confiance essentielle, dont il faut permettre la pleine réalisation, conformément à son mandat.

M. Li Song (Chine) (*parle en chinois*) : Je prends la parole pour exposer la position de la Chine sur les utilisations pacifiques et la sécurité des technologies de l'information et des communications. L'utilisation pacifique de la science et de la technologie, ainsi que la coopération internationale dans ce domaine, constitue un droit inaliénable pour tous les pays. Malheureusement, pendant de nombreuses années, le droit des pays en développement d'utiliser de façon pacifique la science et la technologie et de coopérer librement à l'échelle internationale, a été loin d'être garanti. Le document final du sommet du Mouvement des pays non alignés qui s'est tenu à Bakou a clairement mis en lumière les restrictions déraisonnables auxquelles les pays en développement continuent de se heurter en matière d'exportation de matériaux, d'équipements et de technologies à des fins pacifiques. La Chine estime ainsi qu'il faut répondre à l'appel des pays du Mouvement des pays non alignés, que les droits légitimes des pays en développement en matière d'utilisation pacifique de la science et de la technologie doivent être respectés et que les restrictions injustifiées imposées à ces utilisations doivent être levées dès que possible.

L'année dernière, l'Assemblée générale a adopté la résolution 76/234, intitulée « Promotion de la coopération internationale touchant les utilisations pacifiques dans le contexte de la sécurité internationale », qui a ouvert le dialogue sur les utilisations pacifiques et la coopération internationale en la matière. Conformément à cette résolution, le Secrétaire général a recueilli les avis de toutes les parties et a présenté un rapport (A/77/96) qui a bénéficié d'une très large participation, enregistrant notamment le plus grand nombre de contributions parmi tous les rapports sur le désarmement publiés l'année dernière, ce qui démontre pleinement la volonté générale d'engager un dialogue sur les questions concernées et le besoin pressant qu'un tel dialogue s'ouvre. Cette année encore, la Chine a déposé un projet de résolution sur ce sujet (A/C.1/77/L.56). Tout en adhérant à l'objectif et au concept central de la résolution de l'année dernière, nous avons, dans toute la mesure du possible, tenu compte des propositions de toutes les parties, et visons à poursuivre le dialogue dans le cadre de l'Assemblée générale et à fournir un espace où toutes les parties peuvent discuter des questions pertinentes, des défis et des possibilités de coopération.

Certains pays craignent que l'initiative de la Chine ne cherche à perturber le régime actuel de contrôle des exportations dans le cadre de la non-prolifération. C'est un non-sens absolu. L'antagonisme autour du projet de résolution sur les utilisations pacifiques n'a pas été provoqué par la Chine et ne devrait pas se poursuivre au cours de cette session. Le processus de dialogue mis sur pied sous les auspices de l'ONU, comme le prévoit le projet de résolution, doit au contraire servir de pont pour la communication et le dialogue entre le régime de contrôle des exportations à des fins de non-prolifération et les pays en développement. Je voudrais souligner que la non-prolifération et les utilisations pacifiques ne sont pas des initiatives ennemies, mais bel et bien complémentaires. La Chine appelle les pays en développement à soutenir davantage le projet de résolution, exhorte les pays occidentaux à ne pas entraver le processus de dialogue dans le cadre de l'ONU et appelle les États Membres de l'Organisation des Nations Unies à déployer des efforts concertés pour promouvoir, de manière équilibrée, à la fois les utilisations pacifiques et la non-prolifération, deux objectifs qui, une fois encore, ne s'excluent pas l'un l'autre.

Actuellement, le paysage mondial de la cybersécurité connaît une profonde évolution, avec un énorme déficit en matière de gouvernance cybernétique et numérique, associé à d'importants facteurs d'instabilité et d'incertitude dans le cyberespace. La Chine estime que toutes les parties doivent faire passer l'intérêt général de la communauté internationale avant leurs propres intérêts géopolitiques, l'unité et la coopération avant les divisions et la confrontation. Elles doivent pratiquer un multilatéralisme véritable et définir et observer conjointement des règles internationales consensuelles régissant le cyberespace. Tous les pays, en particulier les grands pays, doivent s'acquitter de leurs obligations internationales avec tout le sérieux qui s'impose, s'engager à construire un cyberespace pacifique, sûr, ouvert et coopératif et observer conjointement, plutôt que de se contenter de mettre en œuvre, le cadre de l'ONU pour un comportement responsable des États dans l'utilisation des technologies de l'information et des communications. Les pays doivent à cet égard s'abstenir d'introduire des différences idéologiques dans le cyberespace, de politiser, d'instrumentaliser et de militariser les

questions scientifiques, technologiques, économiques et commerciales, de fragmenter Internet et de déstabiliser les chaînes d'approvisionnement industrielles.

L'avenir du cyberespace doit être planifié conjointement par tous les pays, que ce soit par l'intermédiaire 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 ou du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation. Les pays conviennent qu'il ne devrait y avoir qu'un seul processus de cybersécurité à l'ONU. Cette année, le groupe de travail à composition non limitée a produit avec succès son premier rapport d'activité annuel (voir A/77/275), ce qui n'est pas un mince exploit dans les circonstances actuelles et démontre la confiance qu'il suscite auprès de toutes les parties.

Toutes les parties doivent se féliciter du dynamisme actuel du groupe de travail et respecter son autorité en tant qu'unique processus de sécurité des technologies de l'information et des communications à l'ONU, conformément à son mandat établi par la résolution 75/240, et entamer des discussions sur la nature du dialogue institutionnel qui sera mené à l'avenir dans le cadre du groupe de travail. Toutes les parties doivent s'abstenir d'essayer d'élaborer un nouveau programme d'action en dehors du groupe de travail et éviter que le processus de cybersécurité de l'Organisation des Nations Unies ne fasse double emploi en suivant des voies parallèles. La Chine travaillera avec toutes les parties pour utiliser pleinement le mécanisme du groupe de travail, renforcer la communication et les échanges et construire ensemble un cyberespace plus équitable, raisonnable, ouvert, inclusif, sûr, stable et dynamique.

M^me^ Lõhmus (Estonie) (*parle en anglais*) : L'Estonie s'associe pleinement à la déclaration faite au nom de l'Union européenne (voir A/C.1/77/PV.18). Je souhaite formuler une série d'observations complémentaires à titre national.

L'Estonie considère indispensables les efforts visant à prévenir et gérer les menaces pour la paix et la sécurité internationales émanant de l'utilisation malveillante du cyberespace. Depuis février, nous assistons à l'agression brutale de la Russie contre l'Ukraine, qui mène, en plus de sa guerre cinétique et de ses campagnes de désinformation, des cyberopérations malveillantes contre les infrastructures critiques et les services essentiels de l'Ukraine. Ces cyberopérations malveillantes menées par la Russie contre le réseau de satellites KA-SAT ont conduit à des coupures de communication et à de graves perturbations au sein des infrastructures privées et publiques de l'Ukraine. Ces attaques ont également touché plusieurs pays tiers, démontrant ainsi la dangereuse ampleur des retombées de ces cyberattaques.

L'Estonie condamne fermement ces cyberopérations malveillantes et les considère comme un mépris délibéré du cadre de l'ONU sur le comportement responsable des États. À cet égard, nous rappelons que le droit international, y compris la Charte des Nations Unies dans son intégralité, le droit international des droits de l'homme et le droit international humanitaire, s'applique pleinement au comportement des États dans le cyberespace. Comme il est indiqué dans le rapport 2021 du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, qui a été adopté par consensus et approuvé par la résolution 76/135, les États Membres sont convenus qu'ils doivent s'abstenir de mener ou de soutenir sciemment une activité numérique qui est contraire aux obligations qu'ils ont contractées en vertu du droit international et qui endommage intentionnellement des infrastructures essentielles ou qui compromet l'utilisation et le fonctionnement d'infrastructures essentielles à la fourniture de services au public.

L'Estonie apprécie grandement le travail du groupe de travail à composition non limitée et se félicite de l'adoption de son rapport d'activité annuel (voir A/77/275) en juillet. Malgré la gravité de la situation géopolitique, ce rapport envoie un signal important sur la nécessité et la volonté des États Membres de poursuivre le débat sur l'élaboration et l'application de normes de comportement responsable des États. Nous encourageons les États à poursuivre des discussions constructives dans cette voie en vue de parvenir à une compréhension mutuelle de la manière d'atténuer efficacement les cybermenaces et de contribuer à renforcer la cyberrésilience au niveau mondial. Afin de faire avancer les discussions sur la mise en œuvre du cadre convenu de comportement responsable des États et de soutenir les efforts de renforcement des capacités, l'Estonie exprime son ferme soutien à l'établissement d'un programme d'action permanent, inclusif et orienté vers l'action. Nous soutenons donc le projet de résolution A/C.1/77/L.73, qui vise à entamer les travaux du programme d'action après l'expiration du mandat du groupe de travail à composition non limitée en 2025 et à s'appuyer sur les travaux de ce dernier, ainsi que sur ceux du précédent groupe de travail et du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale.

Enfin, nous souhaitons souligner le caractère multipartite inhérent au cyberespace et nous nous félicitons de la poursuite de la coopération avec le secteur privé et la société civile. Le haut niveau d'expertise et la diversité des points de vue des différentes parties prenantes permettent de mieux éclairer les discussions sur la cybersécurité au sein de l'Organisation des Nations Unies. L'Estonie estime qu'il est essentiel que ces différentes parties prenantes aient la possibilité d'exprimer leurs opinions lors des prochaines discussions du groupe de travail à composition non limitée.

M. Molla (Bangladesh) (*parle en anglais*) : Le Bangladesh s'associe à la déclaration faite par la représentante de l'Indonésie au nom du Mouvement des pays non alignés (voir A/C.1/77/PV.18).

Le discours sur le désarmement est constamment redéfini par les progrès technologiques, notamment les avancées en matière d'armement émergentes, l'intelligence artificielle et la biotechnologie. En particulier, la révolution des technologies de l'information et de la communication et Internet ont fondamentalement changé notre mode de vie. Certes, la connectivité numérique a révolutionné la vie des êtres humains, mais les risques qu'elle fait peser sur la paix et la sécurité internationales ne doivent pas être sous-estimés. Nous devons donc rester attentifs aux utilisations malveillantes de la technologie qui pourraient mettre en péril notre sécurité collective.

Le cyberespace doit être considéré comme un bien public mondial qui doit bénéficier à tous, partout, sans aucune discrimination. Pour tirer parti des avantages considérables des technologies numériques, la communauté internationale doit mettre en place un environnement numérique sûr, sécurisé, fiable et ouvert, fondé sur l'applicabilité du droit international au cyberespace, sur des normes bien définies de comportement responsable des États, sur des mesures de confiance solides et sur des programmes de renforcement des capacités coordonnés. La cybersécurité est une question de paix et de sécurité internationales et nécessite donc une coopération internationale étroite. Le Secrétaire général identifie également la cyberguerre comme un risque stratégique majeur dans son rapport *Notre Programme commun* (A/75/982). Aucun pays ne peut faire face seul à la menace des cyberattaques. Les États Membres doivent donc créer un climat dans lequel tous les États sont en mesure de profiter pleinement des avantages du cyberespace. Le multilatéralisme est notre seul espoir de créer un environnement numérique libre, sûr, stable, accessible et pacifique. Nous soulignons que l'ONU doit jouer un rôle de premier plan dans l'élaboration de normes internationales applicables au cyberespace.

Le Bangladesh considère que le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, créé par la résolution 73/27, est un mécanisme important et inclusif du système des Nations Unies. Nous réaffirmons notre volonté de contribuer de façon constructive au succès de l'actuel groupe de travail et nous nous félicitons de l'adoption par consensus de son premier rapport d'activité annuel (voir A/77/275), qui, nous en sommes convaincus, servira de feuille de route pour nos futures discussions. Nous soutenons le projet de décision A/C.1/77/L.54, qui a été déposé par Singapour. Nous saluons également le travail accompli par les précédents Groupes d'experts gouvernementaux et leurs rapports, qui contiennent d'importantes recommandations visant à promouvoir un environnement numérique ouvert, sûr, stable, accessible et pacifique.

En l'absence d'une structure normative acceptée au niveau mondial, nous sommes favorables à l'application au cyberespace des principes inscrits dans la Charte des Nations Unies et dans le droit international pertinent afin de maintenir la paix et la stabilité. Au Bangladesh, nous investissons dans la promotion d'une solide culture de la cybersécurité, tant au sein du Gouvernement que de la société. Nous avons mis en place les cadres, les politiques et les stratégies nécessaires et nous les développons en permanence. Nous cherchons à coopérer avec d'autres acteurs à l'échelle internationale, en particulier en ce qui concerne le renforcement des capacités et les mesures de confiance.

Le Bangladesh attache une grande importance à l'intégration et à la préservation des normes environnementales pertinentes dans le régime juridique international concernant le désarmement et la maîtrise des armements. L'applicabilité ou la pertinence de ces normes juridiques aux efforts de désarmement dans les fonds marins et l'espace extra-atmosphérique doit faire l'objet d'études et d'analyses plus approfondies.

Le Bangladesh rappelle également l'importance de l'éducation en matière de désarmement et de non-prolifération. L'éducation joue un rôle fondamental dans la sensibilisation sur les conséquences humanitaires et économiques des armements. Nous tenons à cet égard à exprimer notre reconnaissance envers l'Institut des Nations Unies pour la recherche sur le désarmement pour le travail utile qu'il continue d'accomplir. Nous soulignons la nécessité de garantir à l'Institut la mise à disposition de ressources suffisantes et prévisibles afin qu'il puisse s'acquitter de ses mandats et pour lui permettre d élargir et de gérer sa base de connaissances dans l'intérêt de tous les États Membres.

En conclusion, nous devons placer les êtres humains au centre de nos efforts en matière de désarmement pour que le désarmement permette de sauver des vies, aujourd'hui et demain. Continuons d'œuvrer ensemble à un monde plus sûr.

M. Diack (Sénégal) : Le Sénégal souscrit à la déclaration faite par la représentante de l'Indonésie au nom du Mouvement des pays non alignés (voir A/C.1/77/PV,18) et se réjouit de participer à ce débat thématique sur « Autres mesures de désarmement et sécurité internationale ».

Ma délégation voudrait saisir cette occasion pour partager ses vues sur quelques thématiques inscrites à l'ordre du jour du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Il s'agit particulièrement de l'application du droit international, des mesures de confiance, du renforcement des capacités et de l'instauration d'un dialogue régulier sous les auspices de l'Organisation des Nations Unies.

Concernant l'application du droit international, le Sénégal note que certaines questions comme l'adoption d'un nouvel instrument juridique international ou le maintien du droit international positif pour régir le cyberespace ne sont pas encore résolues. À cet égard, nous estimons qu'il est nécessaire de poursuivre les discussions afin d'éviter les malentendus et de favoriser une meilleure compréhension sur la manière dont le droit international devrait s'appliquer aux activités cybernétiques. Pour le Sénégal, deux aspects méritent une attention particulière.

Le premier est relatif à l'application du droit international humanitaire. Il convient de noter que l'application du droit international humanitaire ne doit pas être interprétée comme une légitimation de la guerre dans le cyberespace, mais plutôt comme une observation stricte des principes de nécessité, de distinction, d'humanité et de proportionnalité dans toutes les cyberactivités menées dans le cadre des conflits armés.

Le second aspect concerne l'application des contre-mesures en réponse à des cyberattaques, y compris les contre-mesures collectives. Sur ce sujet, il est impératif d'aboutir à un consensus propre à garantir un équilibre entre la reconnaissance de leur légalité, notamment pour protéger les pays ne disposant pas de compétences technologiques, et l'encadrement de leur recours afin qu'elles ne soient pas à l'origine de conflits dans le cyberespace. Dans la poursuite de ces discussions, nous sommes favorables au recours à l'expertise d'institutions pertinentes, telles que la Commission du droit international.

S'agissant des mesures de confiance, le Sénégal salue la proposition de mettre en place un répertoire mondial de points de contact nationaux et soutient la recommandation du premier rapport d'activités annuel du groupe de travail invitant à des discussions plus ciblées sur l'opérationnalisation de ce répertoire. Afin de favoriser le partage d'informations, il serait pertinent de travailler sur la modélisation et la standardisation des contributions des États, y compris celles destinées au rapport du Secrétaire général sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, et sur la promotion du comportement responsable des États dans l'utilisation du numérique (voir A/77/92) et au Portail des politiques de cybersécurité de l'Institut des Nations Unies pour la recherche sur le désarmement. Ce modèle pourrait prévoir la communication d'informations sur les politiques de cybersécurité, les cadres juridiques, les structures administratives, les cybermenaces ainsi que les besoins spécifiques en matière de réponses aux cybermenaces.

Cependant, nous devons toujours avoir en ligne de mire les difficultés techniques auxquelles font face certains États. D'où la pertinence du renforcement des capacités, un défi majeur à relever, surtout pour les pays en développement. C'est conscient de cela que le Sénégal s'est doté d'une stratégie nationale de cybersécurité, qui définit cinq objectifs stratégiques : le renforcement du cadre juridique et institutionnel de la cybersécurité ; la protection des infrastructures d'information critiques et des systèmes d'information de l'État ; la promotion d'une culture de la cybersécurité ; le renforcement des capacités et des connaissances techniques en cybersécurité ; et la participation aux efforts régionaux et internationaux de cybersécurité.

Notre pays a consenti des efforts pour adapter le cadre juridique de l'utilisation du numérique et son architecture institutionnelle, notamment avec la création du Service technique central des chiffres et de la sécurité des systèmes d'information, de la Division spéciale de lutte contre la cybercriminalité et de la Commission de protection des données personnelles. Il en est de même du renforcement de la formation sur la sécurité informatique. C'est ainsi que plusieurs établissements de formation ont été mis en place, en particulier l'Institut professionnel pour la sécurité informatique et l'École nationale de cybersécurité à vocation régionale de Dakar, fruit de notre coopération avec la France.

Dans la poursuite de ces efforts, le Sénégal reste attaché à tous les instruments juridiques internationaux pertinents, y compris la Convention de Malabo sur la cybersécurité et la protection des données à caractère personnel, la Convention de Budapest sur la cybercriminalité, la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ainsi qu'à la Directive C/DIR/1/08/11 du 19 août 2011 de la Communauté économique des États de l'Afrique de l'Ouest relative à la lutte contre la cybercriminalité.

Sur l'instauration d'un dialogue régulier sous les auspices de l'Organisation des Nations Unies, ma délégation salue le programme d'action des Nations Unies sur la cybersécurité et le projet de résolution A/C.1/77/L.73 sur sa mise en place. Nous nous réjouissons que les consultations relatives à ce projet aient pris en compte plusieurs préoccupations au nombre desquelles : la reconnaissance du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) comme principal processus de l'Organisation des Nations Unies sur la cybersécurité, le déroulement des discussions sur le programme d'action dans le cadre des travaux de ce groupe et la prise en compte par le programme d'action, une fois opérationnel, des résultats consensuels du groupe.

Ma délégation est convaincue que les mesures de cybersécurité ne doivent pas être édictées à des fins de restriction du développement numérique ou pour freiner l'innovation et les opportunités de développement qu'offrent les TIC. En tant que moyens de prévention et de lutte contre les utilisations malveillantes du cyberespace, ces mesures doivent avoir pour seul but la promotion d'un environnement numérique accessible, sûr, pacifique et prospère, qui ne laisse personne pour compte, conformément à la cible 9c de l'objectif 9 du Programme 2030.

Sur tous ces sujets, le Sénégal réitère sa disponibilité et son engagement au sein du groupe de travail à composition non-limitée seul cadre à même de favoriser des discussions franches et constructives sur la cybersécurité.

M. Zlenko (Ukraine) (*parle en anglais*) : L'Ukraine s'associe à la déclaration faite par l'observatrice de l'Union européenne (voir A/C.1/77/PV.18) et souhaite formuler les observations suivantes à titre national.

Internet a changé sous l'effet des progrès rapides des technologies de l'information et des communications. Aujourd'hui, il ne s'agit plus d'une plateforme de communication confortable, mais d'une véritable arme qui devient de plus en plus dangereuse entre les mains de pirates informatiques, de criminels et de certains acteurs étatiques et de leurs mandataires. Malheureusement, malgré les normes juridiques existantes et les mécanismes institutionnels mis en place pour lutter contre les cyberattaques à l'échelle nationale, régionale et internationale, les avantages du monde numérique moderne n'ont été que trop souvent dévoyés et les cyberattaques de plus en plus fréquemment employées comme une nouvelle méthode de guerre.

Depuis 2014, ces attaques sont l'un des principaux instruments des tentatives externes visant à miner la souveraineté de l'Ukraine. Entre 2014 et 2021, mon pays a fait face à un nombre sans précédent de cyberopérations visant des éléments vitaux de ses infrastructures critiques, plus particulièrement avec le lancement de la cyberattaque à l'aide du logiciel malveillant NotPetya en juin 2017. La plupart de ces attaques ont été menées par des groupes de pirates informatiques contrôlés par la Fédération de Russie. Depuis le début de l'agression militaire russe contre l'Ukraine, le 24 février 2022, les cybercriminels ont attaqué le Gouvernement et les autorités locales. Les institutions commerciales et financières, les secteurs de la sécurité et de la défense, de l'énergie et l'industrie des transports figurent également parmi les principales cibles, et plus précisément toutes les infrastructures qui assurent la subsistance de la population. En fait, l'Ukraine est devenue le premier pays au monde à participer à une véritable guerre cybernétique. Depuis la Seconde Guerre mondiale, l'humanité n'a jamais été confrontée à des défis aussi importants que depuis que la Russie a attaqué notre pays. La guerre est un phénomène totalement nouveau dans le cyberespace. Pendant huit mois de cette guerre, l'équipe d'intervention informatique d'urgence du Gouvernement ukrainien a enregistré plus d'un millier de cyberattaques.

Malgré l'agression militaire russe, l'Ukraine continue de renforcer son système de cybersécurité, notamment grâce à l'assistance matérielle et consultative fournie par ses partenaires. Le système national de cybersécurité que nous avons mis en place dans le cadre de notre stratégie de cybersécurité s'appuie sur le Ministère de la défense, l'Administration nationale chargée des communications spéciales et de la protection de l'information, le Service de sécurité, la Police nationale et la Banque nationale. Il permet la collaboration entre tous les organismes publics, les collectivités locales, les unités militaires, les services de police et de justice, les instituts de recherche et les

établissements d'enseignement, les groupes de la société civile, les entreprises et les autres parties prenantes. La stratégie de cybersécurité de l'Ukraine pour la période 2021-2025 vise à créer les conditions permettant de sécuriser le cyberespace et de veiller à ce que les utilisations qui en sont faites servent les intérêts des individus, de la société et de l'État. Elle repose sur les principes de dissuasion, de cyberrésilience et d'interaction.

Nous soulignons qu'au niveau international, une attention particulière doit être accordée à l'élaboration de normes unifiées pour lutter contre les cybermenaces, au partage des meilleures pratiques, à l'instauration d'une confiance mutuelle dans le domaine de la cybersécurité, à la prévention de l'utilisation du cyberespace à des fins politiques, terroristes et militaires et à la fourniture d'une assistance technique et financière aux États en vue de leur donner les moyens de résister aux cyberattaques, d'atténuer les risques et d'être plus résilients. En outre, la question de l'obligation d'appliquer le principe de responsabilité à tout État ou tout acteur étatique qui se serait rendu coupable de préparer ou de commettre des actes de malveillance informatique ciblés ou de diffuser de fausses informations à des fins hostiles est particulièrement importante. Somme toute, l'action internationale menée dans ce domaine restera vaine en l'absence de mécanismes fiables permettant de repérer, de punir et de traduire en justice les personnes et les États qui coordonnent et financent des activités illicites dans le cyberespace mondial.

En tant que coauteure du projet de résolution A/C.1/77/L.73 qui soutient pleinement l'élaboration d'un programme d'action pour promouvoir le comportement responsable des États dans le cyberespace, qui vise à établir un mécanisme permanent inclusif orienté vers l'action au sein de l'Organisation des Nations Unies, l'Ukraine partage les objectifs clefs de cette initiative, à savoir assurer un soutien aux États dans la mise en œuvre du cadre pour le comportement responsable des États dans le cyberespace et intensifier le dialogue en coopération avec les parties prenantes concernées. À cet égard, notre délégation appuie fermement le projet de résolution A/C.1/77/L.73, déposé par la France.

M. Khaldi (Algérie) (*parle en anglais*) : L'impératif de consolider et de maintenir la paix internationale, la sécurité, la coopération et la confiance entre les États dans l'environnement numérique n'a jamais été aussi clair. En effet, l'évolution des menaces liées à l'utilisation malveillante des technologies numériques, ainsi que le nombre croissant de cyberattaques contre les infrastructures critiques des États, sont très alarmants et nécessitent une réaction collective. Dans ce contexte, l'Algérie ne dira jamais assez qu'il est extrêmement important de veiller à ce que l'utilisation des technologies de l'information et des communications (TIC) respecte pleinement les buts et principes consacrés par la Charte des Nations Unies et le droit international, notamment les principes de souveraineté, d'égalité souveraine, de non-ingérence dans les affaires intérieures, de non-recours à la menace ou à l'emploi de la force dans les relations internationales, de règlement pacifique des différends et de respect des droits de l'homme, et demeure conforme au principe de la coexistence pacifique entre les États.

L'Algérie juge encourageants les progrès concrets qui ont abouti au succès, en 2021, des travaux du groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale. L'adoption par consensus de leurs rapports finaux a donné un élan positif aux actions menées sur le plan multilatéral concernant les TIC dans le contexte de la sécurité internationale et a fourni une base importante pour poursuivre nos délibérations dans ce domaine. Dans ce sens, l'Algérie a soutenu et salué le lancement, sous l'égide de l'ONU, du nouveau groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, créé en application de la résolution 75/240, sous la présidence de Singapour, en tant que seul mécanisme inclusif, basé sur le consensus, avec la participation active et égale de tous les États. Par conséquent, mon pays reste convaincu que le groupe de travail actuel représente une étape importante dans la coopération internationale visant à créer un environnement numérique ouvert, sûr, stable, accessible et pacifique. Bien qu'il reste beaucoup à faire, le nouveau groupe de travail offre une fois de plus un cadre unique dans lequel il est possible non seulement de mieux comprendre les questions cruciales liées à l'évolution des menaces émanant de l'utilisation malveillante des TIC, mais aussi de continuer à travailler collectivement pour relever ces défis.

Nous renouvelons notre ferme soutien au nouveau groupe de travail et notre intention de continuer à travailler de manière constructive avec tous les États Membres pour assurer son succès en 2025, et nous nous félicitons de l'adoption par consensus de son premier rapport d'activité annuel en juillet 2022 (voir A/77/275). Nous espérons sincèrement que l'esprit de consensus prévaudra

au cours des sessions à venir du groupe de travail, qui constituent une importante mesure de confiance. Nous espérons également que les organisations régionales et sous-régionales continueront à jouer un rôle important dans l'accélération de ce processus.

La capacité de la communauté internationale de prévenir ou d'atténuer l'impact d'activités malveillantes liées aux TIC dépend de la capacité de préparation et de riposte de chaque État. Il est donc urgent de mettre en place et de renforcer les capacités des États dans ce domaine.

À cet effet, l'Algérie considère que l'actuel groupe de travail à composition non limitée doit pouvoir déterminer, avant la fin de son mandat, les mécanismes appropriés pour assurer l'assistance et la coopération des États et du secteur privé aux pays en développement, à leur demande. Cette assistance doit également comprendre des ressources financières, des programmes de renforcement des capacités et des transferts de technologie dans les domaines des TIC, tout en tenant compte des besoins spécifiques et des particularités de chaque État bénéficiaire.

Dans le même temps, l'actuel groupe de travail reste le meilleur cadre pour discuter et développer toutes les initiatives pertinentes des États Membres visant à maintenir la paix et la sécurité dans le cyberespace.

Enfin, ma délégation s'associe aux déclarations faites précédemment au nom du Mouvement des pays non alignés et du Groupe des États arabes au titre de ce groupe de questions (voir A/C.1/77/PV.18).

M^me^ Page (Royaume-Uni) (*parle en anglais*) : Le Royaume-Uni s'est engagé à promouvoir le comportement responsable des États dans un cyberespace libre, ouvert, pacifique et sûr.

Depuis de nombreuses années, les États ne cessent de s'inquiéter du fait que les technologies de l'information et des communications (TIC) peuvent être utilisées à des fins incompatibles avec la paix et la sécurité internationales, et que le recours aux TIC dans de futurs conflits entre États est de plus en plus probable.

C'est une réalité. Aujourd'hui, nous voyons la Russie, membre permanent du Conseil de sécurité, recourir à des cybercapacités sophistiquées et à la cyberguerre pour porter atteinte à la paix et à la sécurité mondiales. Nous avons également commencé à voir des États utiliser des cybercapacités dans d'autres conflits à travers le monde.

Le Royaume-Uni se félicite de l'inclusion d'une référence claire et qui fera date à l'applicabilité du droit international humanitaire dans le premier rapport d'activité annuel de consensus du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation. Le monde doit s'unir pour promouvoir l'application et le respect du droit international humanitaire dans les espaces physique et virtuel.

C'est à juste titre que la présidence du groupe de travail à composition non limitée a présenté une décision visant à permettre l'adoption par consensus de son rapport d'activité annuel. Nous appelons tous les États à soutenir cette approche et à rester fidèles au bon travail que nous avons accompli ensemble au cours de la première année d'activité du groupe de travail.

Cependant, bien que nous défendions les résultats de l'actuel groupe de travail, nous ne pouvons pas négliger les défis auxquels nous sommes confrontés pour progresser ensemble. Le Royaume-Uni est une cyberpuissance responsable, qui s'engage à respecter notre cadre commun de comportement responsable des États dans le cyberespace par une action positive.

Premièrement, nous dénoncerons les États qui abuserons du cadre. Au cours des huit derniers mois, nous avons attribué à l'État russe de multiples attaques perturbatrices contre les infrastructures critiques de l'Ukraine, et nous avons constaté une cyberactivité imprudente rendue possible par la République populaire démocratique de Corée, la République islamique d'Iran et la Chine. Une telle activité a des répercussions dans le monde réel. Les effets en cascade sur les infrastructures critiques peuvent s'intensifier et avoir des conséquences potentiellement dévastatrices sur la sécurité, l'économie et la société, ainsi que sur le plan humanitaire.

Nous avons également assisté à des fermetures et à des restrictions d'Internet pour des raisons politiques, ainsi qu'à des perturbations des communications mobiles, lors des récentes manifestations en République islamique d'Iran. Restreindre l'accès des personnes à Internet compromet leur capacité à exercer leurs droits humains, notamment les libertés d'expression et d'association, et leur capacité à demander des comptes aux gouvernements. Nous appelons tous les acteurs étatiques responsables à mettre fin à ces activités malveillantes.

Deuxièmement, tant qu'il sera possible de soutenir la mise en œuvre du cadre et de protéger tous les États contre les activités malveillantes dans le cyberespace, nous le ferons également. Il nous plaît de constater que le groupe de travail a franchi une étape importante dans son appui à l'objectif commun des États Membres, qui est

de faire respecter le comportement responsable des États dans le cyberespace, en élaborant un répertoire mondial d'interlocuteurs.

Enfin, le Royaume-Uni, comme d'autres pays, continuera à développer et à partager sa propre compréhension du cadre, tel qu'il l'a fait récemment dans sa nouvelle déclaration du mois de mai sur la manière dont le droit international existant s'applique à l'activité des États dans le cyberespace. Il s'agit là d'un autre fondement important de notre future collaboration.

Compte tenu du nombre important de questions à traiter, il est clair qu'un dialogue institutionnel régulier est nécessaire à cet égard. Un tel dialogue continuera à se développer au fil du temps, mais il doit être solidement ancré dans le cadre du consensus de base. Par conséquent, nous saluons le projet de résolution déposé par la France (A/C.1/77/L.73), qui prévoit une voie claire et transparente permettant à tous les États Membres de continuer à discuter d'un éventuel futur cyberprogramme d'action au sein du groupe de travail et par le biais de contributions à un rapport du Secrétaire général.

Le dialogue en question doit trouver un équilibre entre la fourniture aux États Membres de l'appui dont ils ont besoin pour mettre en œuvre le cadre et la lutte contre les menaces pesant sur la paix et la sécurité internationales dans le cyberespace, qui sont réelles et qui s'aggravent. Nous ne pouvons négliger les nouveaux défis posés à la paix et à la sécurité dans le cyberespace.

Le Royaume-Uni s'est engagé à approfondir les discussions avec toutes les parties prenantes afin de parvenir à un consensus difficile à atteindre sur des questions complexes. Nous avons encore du chemin à faire. Grâce à une action positive et concrète, nous pouvons remédier au décalage observé entre les actes posés par les pays et leurs engagements à mettre en œuvre le cadre de comportement responsable des États et à faire face aux menaces qui pèsent sur la paix et la sécurité internationales dans le cyberespace.

Pour terminer, je voudrais dire un mot sur les régimes de contrôle de la technologie des missiles, qui constituent un élément critique du système de non-prolifération. En plus de contribuer à la sécurité internationale, ces régimes de contrôle offrent un niveau d'assurance quant à l'utilisation finale, ce qui donne aux États la confiance nécessaire pour transférer des technologies et faciliter les exportations dans le monde entier. Le Royaume-Uni est préoccupé par les efforts que certains États continuent de déployer pour saper et discréditer ces régimes essentiels.

M. Albai (Iraq) (*parle en arabe*) : Tout d'abord, la délégation iraquienne s'associe à la déclaration faite au nom du Groupe des États arabes et à la déclaration faite par la représentante de l'Indonésie au nom des États membres du Mouvement des pays non alignés (voir A/C.1/77/PV.18).

Nous rappelons que la promotion de l'universalité des conventions et traités relatifs au désarmement, notamment ceux qui concernent les armes de destruction massive, au premier rang desquelles les armes nucléaires, est la seule garantie contre leur emploi ou la menace de leur emploi, afin d'éviter les conséquences catastrophiques qui pourraient résulter de l'utilisation de ces armes meurtrières, qui ont une capacité destructrice tant pour l'être humain que pour l'environnement.

Les solutions internationales convenues dans le cadre multilatéral constituent la seule garantie durable pour régler les questions de désarmement et de sécurité internationale. Il est donc nécessaire de réaffirmer et de mettre en œuvre les engagements individuels et collectifs pris dans le cadre multilatéral international. Il faut également que l'ONU joue un rôle central dans le domaine du désarmement et de la non-prolifération.

L'Iraq se déclare de plus en plus préoccupé par la montée en flèche des tensions sur la scène régionale et internationale. Cette situation a contribué à l'utilisation accrue des technologies de l'information et des communications dans des activités qui menacent la paix et la sécurité régionales et internationales. L'Organisation des Nations Unies doit donc continuer à élaborer des règles contraignantes qui contrôlent le comportement responsable des États dans ce domaine, qui est de la plus haute importance. L'ONU doit également continuer à effectuer des contrôles dans ce domaine en fonction de l'évolution rapide de diverses situations.

Par ailleurs, il est nécessaire de poursuivre la coopération internationale tout en préservant le rôle central que joue l'Organisation dans le cadre de ces efforts. À ce titre, l'Iraq se félicite de l'adoption par consensus du premier rapport du groupe de travail à composition non limitée créé par la résolution 75/240 de 2020.

L'Iraq exprime son plein soutien et signale sa volonté de tout mettre en œuvre pour assurer le succès des quatrième et cinquième sessions, prévues l'année prochaine, de manière à adopter des recommandations visant à aider les pays en développement à faire face aux problèmes et aux dangers liés à l'utilisation des technologies de l'information et des communications, en plus des menaces accrues dans ce domaine.

M. Gunaratna (Sri Lanka) (*parle en anglais*) : Sri Lanka s'associe à la déclaration faite par la représentante de l'Indonésie au nom du Mouvement des pays non alignés (voir A/C.1/77/PV.18).

Dans la sphère interconnectée qu'est Internet, nous sommes tous autant en sécurité et aussi vulnérables les uns que les autres, malgré nos capacités différentes. La technologie, dit-on, est un bon serviteur, mais un mauvais maître. Les technologies de l'information et des communications (TIC) se sont révélées être un partenaire de développement essentiel dans de nombreux secteurs pendant la pandémie de maladie à coronavirus (COVID-19). La transformation rapide de l'enseignement est particulièrement importante à cet égard, car elle permet d'atténuer tout échec notable enregistré dans ce secteur.

La pandémie a également modifié le fonctionnement traditionnel des gouvernements et des organisations, en permettant la fourniture de services à distance. Malheureusement, avec ces évolutions, les cyberattaques sont devenues l'une des principales causes de vulnérabilité des infrastructures numériques critiques, entraînant des perturbations dans la prestation de services essentiels, le vol de données sensibles et des fraudes.

Afin de permettre aux pays d'exploiter pleinement les atouts et les avantages liés à l'utilisation des TIC, Sri Lanka rappelle qu'il est important que tous les États Membres prennent des mesures en matière de coopération pour garantir la cybersécurité. Il faut intensifier les actions menées à l'échelle mondiale pour fixer des normes internationales et développer des cadres de gestion des cyberrisques afin de mettre en place une bonne gouvernance et un cadre réglementaire dans le cyberespace. Mon pays prend note avec satisfaction des travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation.

Sur le plan interne, nous mettons en œuvre la première stratégie nationale en matière d'information et de cybersécurité, qui a révélé l'importance d'une approche fondée sur le partenariat pour garantir la cybersécurité. Nous avons continué à renforcer notre cadre juridique pour protéger les utilisateurs d'ordinateurs, les infrastructures nationales critiques et le cyberespace en adoptant la loi sur les délits informatiques, la loi sur la fraude concernant les mécanismes de paiement, la législation sur la protection des données et la loi sur les transactions électroniques. Nous mettons actuellement la dernière main à notre projet de loi sur la cybersécurité.

L'utilisation abusive des TIC par tout acteur, à quelque fin que ce soit, doit être condamnée. À l'ère du numérique, l'utilisation de cette ressource à des fins malveillantes nuit à toutes les structures – sociales, économiques et politiques – et devient davantage un outil de division qu'un pont qui rapproche le monde et nos peuples. L'application de normes, de règles et de principes de comportement responsable et le respect des traités, accords, obligations et engagements dans ce domaine sont, par conséquent, essentiels pour garantir un cyberespace sûr et sécurisé et contribuer à la paix et à la sécurité internationales.

Parallèlement à la dégradation du contexte de sécurité international, nous assistons à une réduction de la coopération consensuelle et de l'orientation des futurs plans d'action dans ce domaine, ce qui est regrettable et préjudiciable à l'ensemble des États. Cette situation ne fera qu'accroître l'utilisation abusive du cyberespace par des terroristes, des extrémistes violents et d'autres acteurs malveillants visant à perturber la sécurité des utilisateurs de cet espace et à menacer la paix et la stabilité internationales.

C'est pourquoi Sri Lanka rappelle l'importance d'une coopération continue, du partage des meilleures pratiques et des capacités entre les pays afin de relever efficacement les défis de la cybersécurité, réduire la fracture numérique et permettre un progrès économique et social sans entrave. Ne redonnons pas vie, dans notre incapacité collective à nous rassembler, aux paroles d'Albert Einstein, prononcées avant l'ère d'Internet, selon lesquelles il était devenu effroyablement évident que notre technologie avait dépassé notre humanité.

M. Hovhannisyan (Arménie) (*parle en anglais*) : L'Arménie s'est engagée à appuyer les efforts déployés par la communauté internationale pour atténuer les risques et faire face aux menaces découlant de l'utilisation des technologies de l'information et des communications (TIC).

La crise provoquée par la pandémie de maladie à coronavirus (COVID-19) a mis en évidence la puissance croissante du numérique pour assurer le fonctionnement correct et continu des gouvernements et la fourniture de services publics et sociaux. Toutefois, les TIC ont également été utilisées pour inciter à la discrimination, à la haine identitaire et pour diffuser une idéologie extrémiste et des pratiques violentes. L'utilisation de plus en plus fréquente des réseaux sociaux pour répandre l'animosité, encourager les crimes de haine pour des motifs ethniques et religieux et glorifier leurs auteurs, en particulier lorsqu'ils sont encouragés au niveau de l'État, constitue une tendance dangereuse qui, si elle n'est pas combattue, pourrait conduire à de graves violations du droit international humanitaire et du droit international des droits de l'homme.

Le quatrième Forum mondial contre le crime de génocide, qui a pour thème « Prévention du génocide à l'ère des nouvelles technologies » et se tiendra en Arménie les 12 et 13 décembre, se concentrera sur les possibilités offertes par les technologies innovantes dans la prévention des atrocités criminelles et les risques découlant de leur militarisation, ainsi que sur l'application d'outils et de plateformes numériques en tant que mécanismes d'alerte rapide pour prévenir la violence et les conflits.

Nous tenons à réaffirmer que les principes et les normes du droit international dans leur intégralité doivent constituer la base d'un comportement responsable des États dans le cyberespace.

Les organisations régionales ont un rôle important à jouer dans la mise en œuvre du cadre pour un comportement responsable des États dans l'utilisation des TIC. À cet égard, l'Arménie apprécie à leur juste valeur les efforts continus déployés dans le cadre de l'Organisation pour la sécurité et la coopération en Europe pour renforcer la transparence, la prévisibilité et la stabilité dans l'utilisation du numérique, ainsi que la pleine mise en œuvre des mesures de confiance prises par cette organisation pour réduire les risques découlant de l'utilisation malveillante des TIC.

Nous soulignons l'importance que revêt le respect des droits humains et des libertés fondamentales dans l'utilisation des technologies numériques. Lorsqu'on étudie les menaces existantes et potentielles dans le domaine de la sécurité du numérique, il est important de ne pas négliger les implications de l'utilisation malveillante des TIC pour la jouissance des droits de l'homme, en particulier le droit de rechercher, de recevoir et de diffuser des informations et des idées sans considération de frontières.

L'Arménie soutient les activités du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, en tant que cadre inclusif et transparent permettant de promouvoir le dialogue entre les États Membres et les autres parties prenantes sur l'application des règles, normes et principes relatifs au comportement responsable des États. Le groupe de travail a pour mission d'examiner l'applicabilité du droit international dans le domaine des TIC, d'identifier les moyens de prévenir et de contrer les menaces dans le domaine de la sécurité du numérique et de promouvoir les mesures de confiance et le renforcement des capacités. Le rapport d'activité annuel des travaux du groupe de travail constitue une bonne base pour faire progresser les discussions entre les États Membres. Nous espérons avoir des délibérations constructives et axées sur les résultats à sa quatrième session de fond, qui se tiendra en mars 2023.

M^me^ Subhashini (Inde) (*parle en anglais*) : Tout d'abord, je souhaite à tous une joyeuse fête de Diwali.

L'Inde a le plaisir de présenter, dans le cadre du groupe de questions que nous examinons, le projet de résolution A/C.1/77/L.59, intitulé « Rôle de la science et de la technique dans le contexte de la sécurité internationale et du désarmement », qui répond au besoin ressenti par les États d'une coopération internationale renforcée touchant les utilisations pacifiques de la science et de la technologie.

Le projet de résolution reconnaît que les nouvelles réalisations scientifiques et techniques peuvent se prêter à des applications aussi bien civiles que militaires et qu'il faut poursuivre et encourager les progrès de la science et de la technique à des fins civiles. Ce projet de texte relève qu'il est nécessaire de réglementer le transfert de technologies à des fins pacifiques, conformément aux obligations internationales correspondantes, afin de lutter contre le risque de prolifération par des États ou des acteurs non étatiques.

Le projet de résolution souligne l'importance pour les États Membres de continuer de s'employer à mettre les progrès de la science et de la technique au service du désarmement et de travailler avec des experts et les parties prenantes concernées de l'industrie, des milieux universitaires et de la société civile pour relever efficacement les défis qui se posent.

L'Inde remercie le Secrétaire général d'avoir présenté le rapport A/77/188 mis à jour, conformément à la résolution 76/24 de 2021. Nous sommes heureux que cette résolution ait été adoptée par consensus et qu'elle ait reçu le soutien de près de 40 États Membres, auteurs et coauteurs, l'année dernière.

En tant que pays en développement, l'Inde est favorable au renforcement de la coopération internationale et à la promotion des utilisations pacifiques de la science et de la technologie par les moyens appropriés, notamment le transfert de technologies, le partage d'informations et l'échange d'équipements et de matériels. Dans le même temps, mon pays estime qu'il est impératif de réglementer efficacement les transferts internationaux de biens et de technologies à double usage et de haute technologie ayant des applications militaires, en gardant à l'esprit les besoins de tous les États en matière de légitime défense et les préoccupations liées à la non-prolifération.

L'évolution rapide de diverses disciplines, notamment les sciences biologiques, les sciences des matériaux, l'intelligence artificielle et l'application des données aux technologies nouvelles et émergentes,

apporte des avantages considérables et peut également poser des défis à la paix et à la sécurité. L'Inde reconnaît la nécessité d'une approche interdisciplinaire pour comprendre leurs implications et formuler des réponses appropriées pour atténuer leurs effets négatifs.

Nous sommes favorables et participons activement aux discussions concernant les technologies émergentes dans diverses instances multilatérales de l'ONU et de ses institutions spécialisées, ainsi que dans le cadre des traités internationaux auxquels nous sommes partie.

L'Inde s'engage à promouvoir un environnement numérique ouvert, sûr, stable, accessible et pacifique. L'utilisation malveillante du cyberespace par des terroristes et à des fins criminelles, ainsi que la nature interconnectée du domaine des technologies de l'information et des communications, nécessitent une approche collaborative, fondée sur des règles, et des travaux visant à garantir l'ouverture, la stabilité et la sécurité du cyberespace.

À cet égard, l'Inde soutient les travaux orientés vers l'action du groupe de travail à composition non limitée sur la sécurité du numérique de son utilisation, présidé par Singapour. Nous nous félicitons de l'adoption par consensus du rapport d'activité annuel 2022 du groupe de travail, qui constitue une base solide pour ses travaux l'année prochaine.

Le groupe de travail, pendant son mandat, doit rester le cadre principal pour toutes les délibérations intergouvernementales sur les questions concernant le numérique liées à son mandat. Nous décourageons fortement la création de processus parallèles formels jusqu'à l'achèvement des activités du groupe de travail.

Consciente des disparités qui existent entre les États Membres en matière de cyberpréparation à la lutte contre diverses cybermenaces et de la nécessité de renforcer leurs capacités, l'Inde a proposé la création d'un portail mondial de coopération en matière de cybersécurité, dont l'ONU serait le point d'ancrage et qui servirait de plateforme mondiale pour le renforcement des capacités et la coopération internationale entre les États Membres. Nous attendons avec intérêt des discussions productives et une décision sur cette question au cours de l'année à venir au sein du groupe de travail.

Compte tenu de la pertinence et de l'importance de ce sujet, il est d'autant plus nécessaire que les États travaillent ensemble pour relever les défis complexes qui se posent. L'Inde sollicite le soutien continu de tous les États Membres en vue de l'adoption par consensus, cette année, de son projet de résolution sur le rôle de la science et de la technique dans le contexte de la sécurité internationale et du désarmement. Nous encourageons également les États Membres à se porter coauteurs du projet de résolution et à se joindre à nous dans cet effort collectif visant à apporter une contribution effective à la paix et à la sécurité mondiales.

M^me^ Rodríguez Acosta (El Salvador) (*parle en espagnol*) : L'interconnectivité croissante et la dépendance à l'égard des technologies de l'information et des communications (TIC) dans tous les domaines de la vie exigent de l'ensemble des États qu'ils s'intéressent davantage aux progrès de la sécurité informatique et qu'ils améliorent leurs connaissances à ce sujet et accordent plus d'importance à la prévention de toute utilisation malveillante du numérique.

Pour ces raisons, mon pays considère la cybersécurité comme un élément fondamental de la sécurité internationale. Nous notons avec inquiétude que les récents incidents impliquant des opérations de logiciels rançonneurs et d'autres types de cyberattaques visant à paralyser ou à ralentir la fourniture de services publics ont eu de graves répercussions sur la sécurité internationale et ont mis en évidence l'urgence de renforcer la cyberrésilience pour nous protéger contre de telles menaces mondiales. C'est un objectif que les États ne peuvent pas atteindre seuls. La coopération active de l'ensemble de la communauté internationale est nécessaire pour relever ces défis.

Nous nous félicitons donc de l'adoption par consensus du premier rapport d'activité du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, auquel nous avons participé activement. Comme l'a indiqué notre délégation dans le recueil d'explications de positions publié lors de l'adoption du rapport, ce dernier ne prétend pas être un résumé exhaustif des travaux du groupe de travail, mais cherche plutôt à mettre en avant les progrès réalisés à ce jour et à donner des orientations pour les discussions futures.

Dans le même ordre d'idées, nous nous félicitons des progrès accomplis dans l'élaboration d'un répertoire mondial d'interlocuteurs, comme l'a mentionné notre délégation lors des dernières sessions de travail du groupe. Nous estimons que cette initiative de renforcement de la confiance pourrait constituer une source précieuse d'échange d'informations sur les menaces, les vulnérabilités et les incidents de cybersécurité en temps réel. Par conséquent, nous avons proposé d'étudier la possibilité de créer ce répertoire aux niveaux technique et opérationnel, parmi les équipes nationales de cybersécurité et les liaisons de cyberdiplomatie.

Nous espérons pouvoir présenter nos contributions nationales avant la quatrième session du groupe de travail. De même, nous prenons bonne note du dépôt du projet de résolution A/C.1/77/L.73, relatif à l'établissement d'un programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. Cette initiative a été soutenue par El Salvador dès le départ. Nous espérons qu'elle complétera les efforts déployés par le groupe de travail actuel et permettra la mise en place future d'un mécanisme de discussion permanent orienté vers l'action pour les États Membres.

Mon pays espère continuer d'œuvrer et de contribuer aux discussions multilatérales visant à renforcer le cadre d'un comportement responsable des États dans le cyberespace et à examiner les menaces réelles et potentielles auxquelles la sécurité et le numérique sont confrontés. Nous réaffirmons donc qu'il est important de progresser vers un cadre contraignant qui permette de protéger les infrastructures critiques et les infrastructures critiques d'information sur les cybermenaces, et de recenser les vulnérabilités en vue de protéger les biens nationaux stratégiques.

El Salvador s'est engagé à faire progresser son programme de transformation numérique en mettant l'accent sur la protection des données personnelles et des infrastructures critiques, afin de renforcer la confiance de la population dans la fourniture de services numériques au niveau national. Nous sommes donc heureux d'avoir mené à bien nos consultations publiques sur la loi relative à la cybersécurité, sous la direction du secrétariat à l'innovation de la présidence du pays. Dans le même ordre d'idées, il est important de continuer à encourager l'élaboration de mesures de confiance qui permettent d'apaiser les tensions et de désamorcer les conflits dans le cyberespace.

Nous avons indiqué avec force l'importance que nous attachons à une large participation des autres parties prenantes à ces processus. Les défis posés par le cyberespace exigent une coopération active de la part de la société civile, des organisations non gouvernementales, des organisations régionales et des milieux universitaires.

Enfin, ma délégation rappelle qu'une approche transversale de la question du genre pourrait nous aider à comprendre la prévalence des types de violence armée et de conflit qui touchent différemment les hommes et les femmes. Nous devons faire preuve de détermination pour relever ces défis. Les questions de genre sont également pertinentes dans le contexte de la cybersécurité internationale.

La version intégrale de la présente déclaration sera disponible sur le portail eStatements.

M^me^ Lee (République de Corée) (*parle en anglais*) : Au cours des deux dernières décennies, l'humanité a connu des progrès sans précédent dans le domaine de la technologie numérique. Si cette évolution nous a apporté des avantages économiques et sociaux comme jamais auparavant, l'augmentation du nombre de personnes recourant au numérique depuis la pandémie nous rend de plus en plus vulnérables aux cyberactivités malveillantes. Le comportement des acteurs étatiques et non étatiques dans le cyberespace complique encore le climat international en matière de sécurité.

Malgré la complexité des défis auxquels nous sommes confrontés, la communauté internationale doit œuvrer de concert à la création d'un cyberespace ouvert, sûr, stable, accessible et pacifique. À cet égard, la République de Corée appuie le rôle central que joue l'ONU dans les discussions en cours visant à répondre aux préoccupations urgentes et à promouvoir un comportement responsable des États dans le cyberespace. Je voudrais notamment mettre en exergue les points suivants.

Premièrement, la République de Corée se félicite du rapport d'activité annuel de 2022 du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, ainsi que de la décision du Président d'approuver ce rapport. Nous continuerons à œuvrer de manière constructive au sein du groupe de travail en nous appuyant sur ce rapport d'activité, adopté par consensus.

En tant que parraine du projet de résolution A/C.1/77/L.73, intitulé « Programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale », déposé par la France, la République de Corée tient à souligner la nécessité de créer un mécanisme permanent dans le cadre de l'ONU, tel que le programme d'action, afin d'améliorer la mise en œuvre concrète des normes et d'encourager l'échange de meilleures pratiques ainsi que le renforcement des capacités.

Deuxièmement, la République de Corée estime que les résultats consensuels obtenus par le groupe de travail et les précédents groupes d'experts gouvernementaux reflètent les progrès accomplis dans le cadre cumulatif et évolutif élaboré pour promouvoir le comportement responsable des États en matière d'utilisation du numérique. En conséquence, comme il ne doit pas y avoir de vide juridique s'agissant du cyberespace, le droit international, notamment la Charte des Nations Unies,

doit lui être appliqué dans son intégralité. En outre, les États doivent respecter et mettre en œuvre fidèlement les normes volontaires et non contraignantes énoncées dans les rapports de consensus des groupes d'experts gouvernementaux et des groupes de travail. En particulier, ma délégation estime que le principe de diligence raisonnable joue un rôle essentiel s'agissant de garantir la cybersécurité, et souhaite coopérer étroitement avec d'autres États Membres pour poursuivre l'élaboration et la mise en œuvre de normes en la matière.

Troisièmement, la République de Corée est un fervent partisan des mesures de confiance et du renforcement des capacités. Les mesures de confiance peuvent limiter le risque de conflit découlant d'un malentendu ou d'une erreur d'appréciation. Nous nous efforcerons également de combler le fossé existant en matière de capacités de cyberdéfense. Nous prenons une part active aux efforts des organisations régionales telles que l'Association des nations de l'Asie du Sud-Est (ASEAN) et le Forum régional de l'ASEAN.

Ma délégation est convaincue que la participation, l'autonomisation et l'éducation de la jeune génération peuvent apporter des contributions précieuses au régime mondial de non-prolifération. Depuis 2019, les États Membres adoptent par consensus une résolution biennale intitulée « Jeunes, désarmement et non-prolifération ». De même, le projet de document final de la dernière Conférence des Parties chargée d'examiner le Traité sur la non-prolifération des armes nucléaires a reconnu l'importance de la diversité des voix et de l'engagement en faveur de l'autonomisation et de la participation des jeunes dans le domaine du désarmement et de la non-prolifération. En tant que championne de l'action 38 du programme de désarmement du Secrétaire général, *Assurer notre avenir commun : un programme de désarmeme*nt, la République de Corée continuera à accompagner le programme et s'engage à maintenir l'élan.

Avant de terminer, ma délégation tient à faire observer que la République de Corée respecte le droit de tous les États Membres d'avoir accès aux matériel, matières et informations scientifiques et technologiques à des fins pacifiques et, dans cet esprit, elle a la ferme conviction que les régimes de contrôle des exportations en vigueur favorisent la réalisation de cet objectif, car ils distinguent ce qui peut être exporté de ce qui ne peut pas l'être, au lieu de donner carte blanche aux pays exportateurs pour des restrictions arbitraires ou des licences injustifiées.

M. Aydil (Türkiye) (*parle en anglais*) : Aujourd'hui, la situation mondiale en matière de paix, de sécurité, de droits de l'homme et de développement économique est de plus en plus influencée par l'utilisation des technologies numériques.

La Türkiye reste préoccupée par l'utilisation malveillante de ces technologies et par l'augmentation du nombre et de la gravité des cyberattaques dans le monde. La vie de nos concitoyens est gravement marquée par des cyberattaques qui visent des infrastructures critiques telles que les communications électroniques, l'énergie, la finance, les transports, la gestion de l'eau et d'autres secteurs essentiels des services publics.

Il est essentiel de s'attaquer à ces menaces et à ces risques pour parvenir à un cyberespace ouvert, libre, stable et sûr au niveau mondial.

De nombreux travaux ont déjà été réalisés concernant le comportement responsable des États dans le cyberespace. Nous soulignons le rôle central que joue l'ONU dans ce processus. À notre avis, les débats sur le cyberespace menés sous les auspices de l'Organisation des Nations Unies ont atteint un certain niveau de maturité. Nous devons donc commencer à discuter de la manière de promouvoir la mise en œuvre du cadre normatif existant.

Le rapport final du précédent groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation a indiqué que le recours aux technologies de l'information et des communications dans les futurs conflits entre États devenait de plus en plus probable. La guerre en Ukraine a justifié cette préoccupation, et la tâche à accomplir est par conséquent urgente.

Pour mieux mettre en œuvre le cadre cumulatif existant, la création d'un programme d'action sur les questions de cybersécurité serait un bon pas en avant. Nous appuyons le projet de résolution A/C.1/77/L.73, déposé par la France à cet effet, et nous nous réjouissons à la perspective de poursuivre nos discussions dans le cadre du programme d'action servant de mécanisme permanent, inclusif et orienté vers l'action. Le programme d'action serait également bénéfique pour la promotion du dialogue et de la coopération sur les questions de renforcement des capacités, qui sont essentielles à la cyberrésilience. Cette initiative ne vise pas à faire double emploi ou à entrer en concurrence avec l'actuel groupe de travail sur la sécurité du numérique et de son utilisation. Elle tiendra compte de ses conclusions et contribuera aux efforts visant à les mettre en œuvre.

La Türkiye participe activement aux travaux de l'actuel groupe de travail. Nous nous félicitons de l'adoption par consensus du rapport d'activité annuel cette année. Nous sommes d'accord avec l'évaluation

selon laquelle le groupe de travail, avec sa composition universelle, est un cadre unique en son genre et constitue en soi une mesure de confiance.

La nature des cybermenaces rend nécessaire une action unifiée. Nous aurions souhaité une approche consensuelle au sein de la Première Commission cette année, comme ce fut le cas l'année dernière. Nous en appelons une fois de plus à un esprit de coopération à cet égard.

M. Ogasawara (Japon) (*parle en anglais*) : Le cyberespace est devenu une infrastructure socioéconomique indispensable à toutes les activités et constitue de ce fait un espace public dans lequel tous les citoyens peuvent se déployer. Cette transformation socioéconomique nous a également rendus vulnérables aux cyberattaques, qui représentent un risque majeur pour la sécurité de tous. S'agissant de la sécurité nationale, nous sommes particulièrement préoccupés par les cyberactivités malveillantes émanant d'autres États qui endommagent les infrastructures critiques, qu'elles soient ou non soutenues par ces États.

Il est difficile pour un pays de faire face tout seul à ces menaces qui pèsent sur la cybersécurité. La coopération et la collaboration entre les États sont primordiales pour protéger et renforcer un cyberespace libre, ouvert et sûr.

En ce qui concerne l'application du droit international aux cyberopérations, la position du Japon est claire, à savoir que le droit international en vigueur s'applique à toutes les opérations de ce type. Nous soutenons également fermement l'élaboration de normes volontaires de comportement responsable de la part des États. La mise en place de l'état de droit au sein de la communauté internationale revêt une grande importance pour la stabilisation des relations entre les pays et le règlement pacifique des différends.

Le Japon considère qu'il est important de promouvoir l'état de droit dans le cyberespace également. Nous estimons que le rapport annuel adopté par consensus au sein du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) permettrait d'y parvenir et de créer un cyberespace libre, équitable et sûr. Comme il s'agit d'un processus orienté vers l'action, il importe que le groupe de travail obtienne des résultats concrets basés sur les conclusions des discussions passées, comme le montrent les rapports du Groupe d'experts gouvernementaux et du groupe de travail. À cet égard, nous soutenons fermement la décision du Président du groupe de travail d'approuver le rapport d'activité annuel.

Nous appuyons également le projet de résolution A/C.1/77/L.73, sur la création d'un programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, déposé par la France.

Je voudrais également aborder la question de l'éducation au désarmement et à la non-prolifération, que mon pays promeut comme un moyen utile et efficace de progresser vers un monde exempt d'armes nucléaires.

À cet égard, il est essentiel que nous sensibilisions le public aux conséquences humanitaires catastrophiques de tout recours aux armes nucléaires, à la menace des divers risques posés par la prolifération de ce type d'armes, ainsi qu'aux mesures nécessaires pour relever ces défis.

L'éducation et la sensibilisation en matière de désarmement et de non-prolifération devraient être menées de manière inclusive et collaborative. Différents acteurs, notamment les établissements d'enseignement et de recherche, les groupes de réflexion, la communauté scientifique, la société civile, le secteur privé, les médias, les municipalités, les organisations internationales et les gouvernements, doivent apprendre les uns des autres et créer des synergies pour faire progresser les initiatives éducatives.

C'est dans cette perspective que le Japon propose de mentionner quelques initiatives concrètes en ce sens au paragraphe 11 du projet de résolution A/C.1/77/L.61, intitulé « Mesures visant à établir un plan d'action commun pour l'avènement d'un monde exempt d'armes nucléaires », qu'il a déposé à la Commission cette année.

Mon pays mène activement diverses actions d'éducation en matière de désarmement et de non-prolifération. Il convient de signaler que, à la Conférence des Parties chargée d'examiner le Traité sur la non-prolifération des armes nucléaires, en août, le Premier Ministre Kishida a annoncé la création du Fonds des jeunes leaders pour un monde exempt d'armes nucléaires. Le Japon a également pris l'initiative de la déclaration commune sur l'éducation en matière de désarmement et de non-prolifération durant la Conférence, laquelle a recueilli le soutien de 89 États parties au Traité.

Nous croyons fermement au pouvoir de l'éducation en matière de désarmement et de non-prolifération et en ce dont les générations futures sont capables pour atteindre notre objectif commun, à savoir l'avènement d'un monde exempt d'armes nucléaires.

Le texte intégral de cette déclaration sera publié sur le site Web du *Journal des Nations Unies*.

M^me^ Romero López (Cuba) (*parle en espagnol*) : Nous nous associons à la déclaration faite par la représentante de l'Indonésie au nom du Mouvement des pays non alignés (voir A/C.1/77/PV.18).

Nous réaffirmons l'engagement de Cuba en faveur d'un désarmement général et complet, qui nous permette de parvenir à un monde exempt d'armes de destruction massive, au bénéfice des générations actuelles et futures. Nous appelons à l'adoption de nouvelles mesures en faveur du désarmement et de la sécurité internationale, qui nous permettent de progresser vers la construction d'un monde de paix.

Nous devons réduire au plus vite les ressources considérables actuellement consacrées aux budgets militaires. Les ressources financières et les progrès scientifiques et technologiques qui servent actuellement à construire le complexe militaro-industriel et à mettre au point, produire et perfectionner des armes de plus en plus meurtrières et sophistiquées apporteraient d'énormes bénéfices à l'humanité s'ils étaient réorientés vers la réalisation d'un développement durable.

Les États Membres doivent continuer à œuvrer à la préservation du multilatéralisme en tant que principe de base des négociations sur le désarmement et la maîtrise des armements. Nous rappelons que ces négociations doivent respecter les normes environnementales internationales en vigueur.

Nous préconisons la négociation d'initiatives juridiquement contraignantes pour empêcher la militarisation de l'espace et du cyberespace, et interdire l'emploi d'armes létales autonomes. Il faut parvenir à des accords réglementant les armes partiellement autonomes et les drones militaires d'attaque.

Nous exprimons à nouveau notre attachement aux travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Nous sommes favorables à des discussions menées sous cette forme, avec la participation équitable de tous les États.

Les technologies de l'information et des communications ne doivent pas être utilisées comme moyen de guerre, mais à des fins exclusivement pacifiques. Nous nous opposons aussi à l'utilisation hostile des télécommunications avec pour objectif avoué ou inavoué de subvertir l'ordre juridique et politique des États ou de commettre ou d'encourager des actes de terrorisme.

Nous rejetons l'emploi de la force comme réponse légitime à une cyberattaque. Nous nous déclarons de nouveau préoccupés par la stratégie cybernétique des États-Unis, qui autorise le recours à des armes cybernétiques et à des opérations cyberoffensives, y compris la possibilité de cyberattaques préventives pour dissuader leurs adversaires.

Nous nous opposons aux méthodes de guerre non conventionnelles que les autorités des États-Unis continuent d'employer contre Cuba, ainsi qu'aux énormes ressources consacrées à cet objectif. Nous condamnons l'utilisation des nouvelles technologies de l'information et d'autres plateformes numériques pour tenter de déstabiliser notre pays, diffuser de fausses informations sur la réalité cubaine et justifier la doctrine de changement de régime à Cuba. Nous dénonçons la création de la « Cuba Internet Task Force », le Groupe de travail sur l'accès à Internet à Cuba, qui viole les normes internationales convenues dans ce domaine. Nous demandons aux États-Unis de lever immédiatement le blocus économique, commercial et financier imposé à Cuba, lequel limite considérablement l'accès du peuple cubain aux technologies de l'information et des communications, ainsi que l'utilisation et l'exploitation de celles-ci pour son bien-être.

Nous sommes convaincus qu'un désarmement général et complet est nécessaire et possible. Mon pays continuera à promouvoir l'adoption de mesures efficaces qui nous permettent d'atteindre ce noble objectif.

M. Salmeen (Koweït) (*parle en arabe*) : La délégation de mon pays s'associe aux déclarations faites au nom du Mouvement des pays non alignés et du Groupe des États arabes, respectivement (voir A/C.1/77/PV.18).

La cybersécurité est l'un des nouveaux problèmes auxquels le monde est confronté, et de nombreux pays en subissent actuellement les effets négatifs, dont l'État du Koweït, qui a essuyé ces dernières années de nombreuses cyberattaques et a été victime d'actes de cyberpiraterie, qu'il s'agisse d'attaques individuelles ou de sabotage commanditées par des groupes terroristes et criminels étrangers. Cette situation résulte du caractère mixte de l'utilisation du cyberespace et du recours à la microtechnologie et aux moyens financiers pour mettre au point de nouveaux systèmes d'armes, ce qui a exacerbé les doutes et la défiance entre les États.

À cet égard, mon pays insiste sur la nécessité de garantir des normes de sécurité et de fournir une protection contre les cyberattaques et les violations programmées. Nous appelons tous les pays à coopérer et à coordonner leurs actions aux niveaux régional et international.

L'État du Koweït accorde une grande importance à la cybersécurité, car il s'agit d'une force défensive essentielle, d'autant plus que non seulement la cybercriminalité vise les individus et les institutions, mais elle met également en péril la sécurité nationale ainsi que les infrastructures et les économies des États. C'est la raison pour laquelle l'État du Koweït a lancé une stratégie nationale de cybersécurité pour la période 2017-2020 afin de renforcer la culture de la cybersécurité et de promouvoir l'utilisation équitable et sûre du cyberespace koweïtien, ainsi que de protéger les infrastructures informatiques nationales critiques, notamment en renforçant les mécanismes d'échange d'informations entre les différentes parties prenantes, tant locales qu'internationales. Nous soulignons que notre stratégie est conforme aux politiques de sécurité strictes et aux critères mondiaux qui assurent la protection des informations contre tous les types de piratage et garantissent un cyberespace koweïtien sûr et durable.

Dans ce contexte, étant donné que les dirigeants politiques koweïtiens sont conscients de l'ampleur des défis que nous impose le cyberespace, et en raison de l'attachement de mon pays à la transformation numérique pour promouvoir notre développement national dans le cadre du nouveau Koweït 2035, l'État du Koweït a créé un centre national de cybersécurité qui comprend un centre des opérations de sécurité informatique ainsi qu'une équipe de gestion des urgences cybernétiques, en vue de mettre en place une stratégie nationale globale de sécurité du cyberespace. Cela garantira la protection de nos réseaux d'information et de télécommunication et permettra la collecte et l'échange d'informations par l'utilisation de tout dispositif électronique, en partenariat avec toutes les parties prenantes nationales.

Nous sommes témoins d'une révolution technologique et d'une transformation numérique accélérée et sans précédent, et nous avons recours de plus en plus à Internet et aux moyens de communication modernes. Le monde est aujourd'hui plus interconnecté que jamais, ce qui accroît le risque de cyberattaques, notamment de vols d'informations et de violations de la confidentialité. Il y a également des failles importantes dans les armements modernes, qui dépendent de la technologie. Dans ce contexte, l'État du Koweït est préoccupé par les armes autonomes et l'impression 3D dans le domaine des télécommunications, qui s'est répandue dans les processus de fabrication à travers le monde. Il s'agit là d'une nouvelle menace pour la paix et la stabilité internationales, si ces technologies devaient tomber entre les mains de groupes terroristes ou de groupes criminels organisés ou être utilisées illégalement, ce qui aurait certainement des conséquences désastreuses pour les infrastructures concernées et le flux de produits fabriqués en toute sécurité. À cet égard, mon pays réaffirme sa position inébranlable concernant le désarmement et la sécurité internationale. Nous pensons que la circulation et la prolifération des armes vont à l'encontre de l'objectif que nous nous sommes fixé, à savoir la paix et la stabilité internationales.

Nous appelons par conséquent tous les États à déployer des efforts pour parvenir à un instrument international contraignant et consensuel qui régirait l'utilisation du cyberespace et à créer des mécanismes d'échange d'informations entre les États parties. En outre, un tel instrument doit respecter la souveraineté des États en ce qui concerne les drones, qui sont largement utilisés comme un nouveau moyen de guerre ciblant les civils et les infrastructures des États. Nous exprimons à nouveau notre condamnation de toutes les attaques cybernétiques et électroniques impliquant l'utilisation de drones, car elles ont de graves répercussions sur la sécurité aux niveaux régional et international. Dans ce contexte, nous appelons les États à respecter les principes consacrés par la Charte, notamment les relations de bon voisinage, le respect de la souveraineté des États et la non-intervention dans leurs affaires intérieures.

L'État du Koweït se félicite des deux programmes d'action sur la cybersécurité lancés par le Secrétaire général António Guterres dans le cadre du Programme de désarmement de 2018.

Pour terminer, nous saluons toutes les actions menées sur le plan international concernant la question de la cybersécurité et appelons à ne pas les politiser et à promouvoir le principe de transparence à cet égard. Nous soulignons que nous continuons à soutenir toutes les mesures internationales qui renforcent la confiance et les capacités afin de limiter les menaces qui pèsent sur la paix et la sécurité internationales.

M. Jotterand (Suisse) : La Suisse est préoccupée par le recours accru aux cyberopérations dans le cadre du conflit armé en cours en Ukraine, en particulier si elles sont dirigées contre des infrastructures critiques. Le potentiel de conséquences involontaires ou d'effets de débordement est ainsi accru. La Suisse exhorte toutes les parties au conflit armé à respecter le droit international humanitaire et le droit international des droits de l'homme. Cela s'applique également au cyberespace.

Dans notre monde en mutation rapide, les utilisations civiles et militaires du cyberespace se multiplient, posant de nouveaux défis pour la paix et la sécurité

internationales. Ces nouveaux défis ne peuvent être relevés que par le respect du cadre convenu du comportement responsable des États dans le cyberespace. Comme l'ont confirmé les rapports consensuels du Groupe d'experts gouvernementaux et du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), ce cadre comprend l'application du droit international dans le cyberespace, la mise en œuvre des 11 normes volontaires, ainsi que des mesures de confiance et le renforcement des capacités.

Nous nous félicitons de l'adoption par consensus, en juillet 2022, du rapport d'activité annuel du groupe de travail à composition non limitée. Ce rapport contient, entre autres éléments, d'importantes propositions visant à clarifier davantage l'application concrète du droit international, y compris le droit international humanitaire, et la mise en œuvre de normes volontaires sur le comportement responsable des États dans le cyberespace.

Le travail critique en cours de l'actuel groupe de travail offre une occasion précieuse de poursuivre le consensus sur l'application du droit international dans le cyberespace. Pour contribuer à notre objectif commun de créer une compréhension commune de la manière dont le droit international s'applique au cyberespace, la Suisse a publié en 2021 sa position nationale sur cette question importante.

Nous encourageons tous les États Membres de l'ONU à envisager de publier leur propre position nationale. Par ailleurs, nous nous réjouissons de poursuivre les délibérations sur tous les éléments du mandat de l'actuel groupe de travail à composition non limitée.

Nous saluons la proposition du Président du groupe de travail à composition non limitée de tenir des consultations intersessions en 2023 et 2024 pour faire avancer les discussions, s'appuyer sur le rapport d'activité annuel et soutenir la poursuite des travaux de ce groupe. À cet égard, nous remercions le Président du groupe de travail d'avoir présenté à la Commission un projet de décision (A/C.1/77/L.54) qui englobe à la fois l'approbation de ce rapport ainsi que les consultations intersessions que j'ai mentionnées. La Suisse soutient pleinement le projet de décision et cette approche purement procédurale et pratique.

Nous devons également souligner que nous avons de fortes interrogations concernant le projet de résolution (A/C.1/77/L.23/Rev.1) déposé par la Fédération de Russie sur cette question, car il semble à la fois inutile et faire double emploi avec le texte du Président du groupe de travail à composition non limitée. Le projet déposé par la Russie soulève également des questions de fond, notamment parce qu'il ne s'appuie pas sur un langage consensuel et utilise une approche sélective. Cela risque de remettre en question les progrès importants réalisés jusqu'à présent dans l'actuel groupe de travail. En l'état actuel, la Suisse ne serait pas en mesure de soutenir ce projet.

La mise en place d'une plateforme pour un dialogue institutionnel régulier sur le cyber au sein de l'ONU mérite également toute notre attention. La Suisse souhaite souligner que les décisions sur l'avenir des discussions sur le cyber à l'ONU doivent être basées sur des délibérations inclusives qui permettent à tous les États Membres de présenter leurs points de vue. De plus, selon nous, tout processus futur de l'ONU doit se concentrer sur le soutien des États Membres dans leurs efforts pour mettre en œuvre le cadre existant pour un comportement responsable des États dans le cyberespace.

Il est important de s'appuyer sur ce qui a été réalisé ces dernières années, de le préserver et d'utiliser efficacement les recommandations convenues. C'est pourquoi nous soutenons le projet de résolution A/C.1/77/L.73, sur un programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, déposé par la France, qui permettra aux Membres de l'ONU de faire avancer cette discussion.

M^me^ Vladescu (Roumanie) (*parle en anglais*) : La Roumanie s'associe pleinement à la déclaration faite par la représentante de l'Union européenne (voir A/C.1/77/PV.18) et souhaite formuler les observations suivantes à titre national.

Nous nous réunissons dans un environnement de sécurité fondamentalement modifié, marqué par des tensions accrues et des défis mondiaux qui continuent d'éroder le dispositif de maîtrise des armements, de désarmement et de non-prolifération. L'agression militaire illégale, injustifiée et non provoquée de la Fédération de Russie contre son voisin, l'Ukraine, nous a fait entrer dans une phase d'escalade sans précédent.

Depuis le 24 février, nous assistons aux conséquences tragiques de cette agression, au cours de laquelle la Russie a utilisé tous les types d'armes classiques ainsi que la désinformation et les cyberattaques. La Roumanie condamne résolument l'agression russe et réaffirme son soutien indéfectible à l'indépendance, à la souveraineté et à l'intégrité territoriale de l'Ukraine à l'intérieur de ses frontières internationalement reconnues.

La sécurité du cyberespace est devenue une question hautement prioritaire étant donné que les activités malveillantes liées aux technologies de l'information

et des communications menées par des acteurs qui représentent une menace permanente, parmi lesquels se trouvent des États et d'autres parties prenantes, peuvent créer un risque important pour la sécurité et la stabilité internationales, pour le développement socioéconomique ainsi que pour la sécurité et le bien-être des personnes.

Aujourd'hui plus que jamais, il est important de promouvoir un cyberespace ouvert, sûr, stable, accessible et pacifique, d'adhérer pleinement au cadre des Nations Unies pour un comportement responsable des États et de poursuivre notre travail de contribution à la sécurité et à la stabilité dans l'utilisation des technologies de l'information et des communications (TIC) par les États.

La Roumanie se félicite du consensus obtenu cette année sur le rapport d'activité annuel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), créé par la résolution 75/240. Nous réaffirmons notre soutien sans réserve à la décision du Président du groupe de travail à composition non limitée sur la question et son appel à une adoption consensuelle.

Nous encourageons tous les États Membres à soutenir le projet de résolution A/C.1/77/L.73, sur un programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, coparrainé par un groupe transrégional d'États et qui bénéficie du plein soutien de la Roumanie.

En ces temps de tensions et de conflits accrus, la nécessité de renforcer la transparence, en particulier dans le domaine des dépenses militaires, est encore plus pertinente. À cet égard, nous voudrions appeler l'attention sur le projet de résolution de cette année intitulé « Information objective sur les questions militaires, y compris la transparence des dépenses militaires » (A/C.1/77/L.63), traditionnellement déposé par la Roumanie et l'Allemagne. Nous demandons instamment aux États Membres de l'ONU d'appuyer le projet de résolution, qui repose sur le principe central du renforcement de la confiance entre les États.

Le système des Nations Unies pour l'établissement de rapports normalisés sur les dépenses militaires a connu un succès remarquable pendant de nombreuses années et devrait rester l'un de nos outils les plus importants pour renforcer la transparence. Nous saisissons cette occasion pour souligner une nouvelle fois l'importance que continue de revêtir le Rapport des Nations Unies sur les dépenses militaires, d'autant plus dans les circonstances actuelles, et nous encourageons tous les États à participer activement à l'établissement de ce rapport.

Étant donné qu'aucune évolution notable n'a été enregistrée en ce qui concerne le système pour l'établissement de rapports normalisés depuis l'adoption en 2019 de la résolution précédente sur la question, la résolution 74/24, en raison également de la pandémie de maladie à coronavirus (COVID-19), nous avons choisi de conserver le texte tel qu'il a été adopté précédemment par la Première Commission et l'Assemblée générale et de proposer une prorogation technique avec seulement quelques mises à jour techniques mineures. Cette résolution figure à l'ordre du jour de la Première Commission depuis plus de 20 ans et a toujours bénéficié d'un soutien massif de la part des États Membres de l'ONU. Nous espérons qu'à la présente session, le projet de résolution recevra le même accueil et que les États Membres manifesteront à nouveau leur soutien en l'adoptant sans vote, comme cela a été le cas à de nombreuses reprises lors des sessions précédentes de la Première Commission.

M. Vidal (Chili) (*parle en espagnol*) : Le Chili s'associe à la déclaration faite par la représentante de l'Indonésie, au nom du Mouvement des pays non alignés (voir A/C.1/77/PV.18).

Nous accueillons favorablement les textes fondés sur l'égalité et l'équité entre les sexes et qui promeuvent les droits humains des femmes, des enfants et des personnes différentes dans les forums multilatéraux et les organisations internationales, ainsi que les textes qui prennent en compte les questions de genre dans ces négociations.

À cet égard, nous saluons le projet de résolution A/C.1/77/L.18, intitulé « Femmes, désarmement, non-prolifération et maîtrise des armements », déposé par la Trinité-et-Tobago et coparrainé par mon pays. Il est impératif de faire référence aux questions de genre, telles qu'elles figurent dans les mandats existants des Nations Unies, en particulier dans le domaine de la sécurité internationale. Les questions de genre doivent être traitées dans le cadre d'un processus inclusif, équitable et efficace.

Le Chili estime que les menaces posées par les technologies de l'information et des communications (TIC) peuvent toucher les États différemment, en fonction de leur niveau de numérisation, de capacité, de sécurité et de résilience en matière de TIC, ainsi que de leur infrastructure et de leur développement. Ces menaces peuvent également avoir des effets différents sur divers groupes et entités, en particulier les femmes et les filles. Les États tels que le nôtre sont confrontés à différents types de menaces et de besoins. Il est donc essentiel de renforcer nos capacités de créer des structures et des plans de coordination, non seulement au niveau gouvernemental, mais aussi en développant des partenariats efficaces avec la société civile, le secteur privé et le monde universitaire.

Le Chili estime que le droit international, en particulier la Charte des Nations Unies, constitue le cadre normatif applicable qui doit régir le comportement des États dans le cyberespace, y compris le droit international humanitaire, les droits de l'homme et les lois qui régissent la responsabilité internationale des États, car ils sont essentiels au maintien de la paix et de la stabilité nécessaires à la promotion d'un environnement ouvert, sûr, stable, accessible et pacifique pour les technologies de l'information et des communications.

Pour toutes ces raisons, nous soutenons les travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), dirigé par le Représentant permanent de Singapour, ainsi que le programme d'action visant à promouvoir un comportement responsable des États dans l'utilisation des TIC dans un contexte international. Notre pays, comme les autres Membres, soutiendra toujours les textes qui renforcent la confiance. Nous soutenons toutes les instances au sein desquelles les États peuvent échanger leurs points de vue et exprimer leurs priorités et leurs besoins, renforçant ainsi la sécurité, la résilience et l'utilisation pacifique des TIC en général.

M. Soares Damico (Brésil) (*parle en anglais*) : Dans *Assurer notre avenir commun : un programme de désarmement*, le Secrétaire général a réaffirmé la nécessité de ramener la relation entre le désarmement et le développement au premier plan de la conscience internationale.

Conformément à la position adoptée de longue date par les pays en développement, le Brésil partage l'idée évidente qu'il existe une corrélation positive entre le désarmement et le développement. En effet, la sécurité nationale et internationale est un élément essentiel de la croissance économique. Si les ressources financières et technologiques investies dans l'expansion des arsenaux classiques et stratégiques avaient été réorientées vers des secteurs cruciaux de la vie humaine tels que l'éducation, les soins de santé et la protection de l'environnement, nous nous en serions beaucoup mieux portés. Le lien entre le désarmement et les objectifs de développement durable doit donc être au cœur-même de nos efforts.

Les dividendes de la paix que nous avons récoltés sont considérables. En 1960, les dépenses militaires moyennes s'élevaient à 6,3 % du produit intérieur brut (PIB). Soixante ans plus tard, ce chiffre a atteint son niveau le plus bas : 2,4 %. Cela signifie que dans 25 ans, nous pourrions compter sur une année de PIB pour améliorer le bien-être social.

Néanmoins, les tensions actuelles ont entraîné un renversement spectaculaire de cette tendance. Pour ne rien arranger, cela a coïncidé avec une période de déficits publics sans précédent, qui, dans certains pays développés, ont atteint des niveaux qui n'avaient été observés que pendant la Seconde Guerre mondiale, en raison de la lutte contre les conséquences de la pandémie de maladie à coronavirus (COVID-19). La seule consolation que nous pouvons tirer de cette situation est que, dans un avenir assez proche, les contribuables seront contraints de trancher le dilemme entre le beurre et les armes.

Le désarmement, la non-prolifération et la maîtrise des armements ne peuvent plus rester confinés à la haute politique. Plus que jamais, ils reflètent des choix de société, compte tenu de leur impact considérable sur la vie quotidienne de millions de personnes partout dans le monde, chaque jour.

Notre programme de désarmement actuel englobe une nouvelle variété de sujets plus proches de nos réalités, tels que les considérations de genre, les discussions sur le libre accès aux technologies à des fins pacifiques et les aspects sécuritaires des technologies de l'information et des communications. Cette proximité ne rend cependant pas ces sujets moins complexes. Un grand fossé persiste quant à la manière de les traiter.

Le Brésil estime que le débat sur les technologies sensibles et émergentes occupe une place prépondérante dans les relations internationales actuelles. Les questions de sécurité ne doivent pas seulement être abordées avec soin ; nous devons également plaider en faveur d'un environnement ouvert, accessible, pacifique et sûr pour le développement, l'échange et l'utilisation de ces technologies. La priorité est de trouver un équilibre délicat dans le traitement de ce sujet afin de sauvegarder les avantages socioéconomiques incontestables que les technologies apportent à nos peuples et de freiner leur utilisation malveillante par des États ou des acteurs non étatiques. Cette approche protège le droit légitime de tous les États d'avoir accès à des technologies cruciales pour leur développement, tout en préservant les objectifs légitimes de non-prolifération et de sécurité internationale.

Le développement des technologies de l'information et des communications (TIC) est devenu un sujet de discussion central des sessions de la Première Commission. Depuis 1998, six groupes d'experts gouvernementaux ont été convoqués, dont deux présidés par le Brésil.

Cet engagement continu des Membres à maintenir la question des TIC à l'ordre du jour illustre sa nature stratégique et l'urgence d'une réglementation appropriée

visant à préserver le cyberespace en tant qu'environnement ouvert, pacifique et accessible, ainsi que la nécessité d'empêcher le cyberespace de devenir le théâtre d'un conflit.

Dans cette optique, il est essentiel de concilier les différentes visions du rôle joué par le cyberespace dans nos sociétés et de ce que nous en attendons. De par sa nature même, cet exercice intergouvernemental bénéficierait des contributions émanant de la société civile, du monde universitaire et de l'industrie. Néanmoins, la base de cette discussion repose sur l'applicabilité du droit international, en particulier de la Charte des Nations Unies, et sur la protection intransigeante des droits de l'homme.

Nous espérons que l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation et le futur mécanisme de dialogue institutionnel qui sera établi par la suite renforceront les notions de comportement responsable, la transparence et les mesures de confiance, ainsi que le renforcement des capacités, en capitalisant sur le travail effectué par les précédents groupes d'experts gouvernementaux et reflété dans les rapports du groupe de travail à composition non limitée adoptés par consensus.

Nous ne pouvons manquer de souligner le travail réalisé par l'Ambassadeur Burhan Gafoor, de Singapour, en tant que Président du groupe de travail à composition non limitée sur la sécurité sur la sécurité du numérique et de son utilisation. Nous nous félicitons de l'adoption du rapport annuel lors de sa dernière session. Il constitue une bonne base pour la poursuite de nos travaux.

M. Sánchez Kiesslich (Mexique) (*parle en espagnol*) : Les défis transversaux liés à la sécurité internationale exigent des mesures intégrales qui vont au-delà des conceptions traditionnelles de la sécurité. C'est pourquoi nous soulignons l'importance de toutes les mesures qui renforcent les cadres régionaux et internationaux existants en matière de sécurité internationale, de maîtrise des armements, de désarmement et de non-prolifération.

Les utilisations légitimes et pacifiques du cyberespace, la résilience numérique et les possibilités offertes par les technologies de l'information en tant qu'instruments du développement durable ne peuvent être maintenues et garanties que par des moyens multilatéraux. L'attention croissante et continue de la Première Commission à ce sujet témoigne clairement de notre confiance dans le rôle prioritaire de l'Organisation des Nations Unies et du multilatéralisme. Les attentes sont grandes, mais les menaces et les défis seront encore plus grands si nous ne parvenons pas à garantir une architecture pour l'environnement numérique du futur.

Ma délégation salue les progrès accomplis en vue de la prise en compte des questions de genre dans diverses résolutions de l'ONU et dans les traités multilatéraux liés à la Première Commission. Comme d'autres délégations, nous pensons que la participation pleine, égale et véritable des femmes aux efforts de désarmement et de non-prolifération est indispensable pour parvenir à une paix durable. Nous continuerons à promouvoir et à soutenir les initiatives visant à accroître la participation des femmes aux processus décisionnels dans ce domaine. C'est pourquoi, cette année, comme par le passé, nous sommes heureux de nous porter coauteurs du projet de résolution A/C.1/77/L.18 intitulé « Femmes, désarmement, non-prolifération et maîtrise des armements ».

De même, le Mexique reste fermement attaché à l'éducation au désarmement en tant que moyen de prévention. Nous pensons que cette stratégie favorise la prise de conscience de l'impact de l'utilisation de tout type d'arme sur la société et notre environnement. Elle forme également les jeunes générations intéressées à devenir de nouveaux agents de changement dans les domaines du désarmement et de la sécurité internationale.

Cette année encore, nous avons le plaisir de déposer des projets de résolution bisannuels sur le Programme d'information des Nations Unies sur le désarmement (A/C.1/77/L.20) et l'étude de l'Organisation des Nations Unies sur l'éducation en matière de désarmement et de non-prolifération (A/C.1/77/L.15). Nous espérons que ces projets recevront le soutien de toutes les délégations.

Enfin, nous sommes heureux de voir trois Mexicains participer à l'initiative « #Leaders4Tomorrow », et nous espérons que ces projets exemplaires toucheront beaucoup plus de jeunes afin qu'ils puissent diffuser des informations sur l'importance du désarmement dans leurs propres communautés.

M. Tun (Myanmar) (*parle en anglais*) : Le Myanmar s'associe aux déclarations faites au nom du Mouvement des pays non alignés et de l'Association des nations de l'Asie du Sud-Est (voir A/C.1/77/PV.18).

Il ne fait aucun doute qu'en l'absence des technologies de l'information et des communications (TIC), divers aspects de notre vie s'arrêteraient. La croissance exponentielle des TIC nous a permis de saisir des possibilités de développement socioéconomique sans précédent, qui profitent à tous dans le monde entier, y compris à ceux qui n'ont pas accès aux TIC ou qui n'en ont qu'une compréhension très limitée.

Dans le même temps, le cyberespace devient de plus en plus vulnérable aux acteurs malveillants et aux acteurs non étatiques dont les capacités complexes se développent au

même rythme que les TIC elles-mêmes. Les cybermenaces omniprésentes, transfrontalières, insaisissables et évolutives, ont de graves conséquences sur la paix et la sécurité internationales et sur notre vie quotidienne. Le cyberespace est déjà devenu un forum de guerre, comme nous l'avons vu au cours des deux dernières décennies.

Il est donc impératif pour nous tous d'utiliser les normes internationales comme guides pour réduire au minimum les cybermenaces et maximiser les avantages des TIC. À cet égard, le Myanmar souhaite souligner le rôle principal de l'ONU et les efforts multilatéraux des États Membres pour relever les défis de la cybersécurité et construire un environnement de sécurité sûr et stable. En conséquence, le Myanmar renouvelle son soutien aux travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et se félicite de l'adoption par consensus du premier rapport d'activité annuel en juillet 2022.

Nous appelons toutes les parties à travailler ensemble de bonne foi et avec un maximum de souplesse pour que le groupe de travail puisse continuer à aller de l'avant. Nous apprécions également beaucoup le travail important du Groupe d'experts gouvernementaux, qui a apporté une contribution précieuse dans ce domaine.

Nous condamnons l'utilisation des TIC comme arme pour supprimer les droits fondamentaux et la liberté d'expression. Au Myanmar, mon pays d'origine, un Internet libre, sécurisé et ouvert n'est plus possible, car la junte militaire exerce une dictature numérique. Les écoutes téléphoniques et les cyberattaques contre son propre peuple, y compris les ressortissants du Myanmar vivant à l'étranger, sont devenues la nouvelle norme. La junte a activement surveillé les activités des fonctionnaires sur les médias sociaux. La junte tente également de promulguer une loi draconienne sur la cybersécurité qui est spécifiquement conçue pour éliminer toute dissidence ou expression contre la junte militaire. Nous demandons instamment à la communauté internationale et à l'industrie technologique de contribuer à mettre un terme à l'utilisation abusive des TIC par la junte pour s'accrocher au pouvoir.

Je saisis cette occasion pour appeler votre attention, Monsieur le Président, sur les crimes odieux commis récemment par le régime militaire fasciste contre les minorités ethniques kachin. Dans la soirée du 23 octobre, des avions de combat de l'armée terroriste ont bombardé et attaqué un concert de musique organisé à A Nang Pa, brigade 9 de l'Armée de l'indépendance kachin, dans l'État kachin, au Myanmar, pour célébrer le soixante-deuxième anniversaire de l'organisation indépendante kachin, qui tombe le 25 octobre. Ces attaques auraient entraîné la mort d'une centaine de personnes, dont des artistes, des femmes et des enfants, et fait de nombreux blessés. Cela constitue de toute évidence un crime contre l'humanité et un crime de guerre. Il ne s'agit pas d'un incident isolé. Au cours des 20 derniers mois, l'armée terroriste a mené plus de 250 frappes aériennes contre la population civile dans tout le pays, y compris dans les zones ethniques, et a commis plusieurs massacres. Tant que l'armée conservera son accès aux armes et aux technologies, elle continuera à commettre des atrocités graves et inhumaines contre la population, y compris les enfants. Je demande aux États Membres qui exportent des armes et des technologies mortelles vers l'armée d'y mettre fin immédiatement. Nous estimons que cela sauvera la vie des habitants du Myanmar.

En conclusion, nous réaffirmons notre engagement en faveur d'un cyberespace sûr et pacifique qui empêche les activités néfastes portant atteinte à la paix et à la sécurité internationales et qui favorise l'application du droit international, des libertés fondamentales et des droits de l'homme.

M. Balouji (République islamique d'Iran) (*parle en anglais*) : Ma délégation s'associe à la déclaration faite par la représentante de l'Indonésie au nom du Mouvement des pays non alignés (voir A/C.1/77/PV.18).

La République islamique d'Iran réaffirme une fois de plus sa position constante selon laquelle le cyberespace et l'environnement des technologies de l'information et des communications (TIC), en tant que patrimoine commun de l'humanité, doivent être utilisés à des fins exclusivement pacifiques, et les États doivent agir en coopération et dans le plein respect du droit international applicable. C'est pourquoi l'Iran participe activement aux négociations intergouvernementales qui sont conduites à ce sujet sous les auspices des Nations Unies dans l'intérêt des droits de tous, tout en établissant également les responsabilités qui reviennent à chacun. Après l'adoption du premier rapport annuel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation et d'un recueil de déclarations des États Membres expliquant leur position, y compris une déclaration de l'Iran, nous pensons que la poursuite des progrès et l'amélioration de l'efficacité du Groupe dépendront des éléments suivants.

Premièrement, il est essentiel, dans les discussions futures, d'examiner et d'arrêter la liste non exhaustive et diversifiée des propositions faites sur l'élaboration de règles, de normes et de principes de comportement responsable des États, comme indiqué dans le résumé du Président figurant dans le rapport de 2021 du groupe de travail à composition non limitée.

Deuxièmement, conformément au mandat du groupe de travail à composition non limitée, un dialogue institutionnel régulier doit être instauré sous les auspices des Nations Unies, avec une large participation des États. À cet égard, toutes les initiatives nationales doivent être traitées sur un pied d'égalité, tout en prenant en compte les préoccupations et les intérêts de tous les États.

Troisièmement, nous appelons les États à continuer à prendre une part constructive dans les négociations au cours des activités ultérieures du groupe, y compris pendant l'intersession.

Quatrièmement, nous demandons au groupe de travail à composition non limitée de créer, conformément à son mandat, des sous-groupes thématiques pour remplir celui-ci, faciliter les échanges de vues entre les États et élaborer des rapports ultérieurs par le biais de négociations fondées sur des textes. D'un autre point de vue, et compte tenu des réalités sur le terrain, il importe de noter que des pays comme les États-Unis ont non seulement commencé à militariser le cyberespace, mais que leurs armées ont également commencé à mener de multiples cyberattaques. Le régime israélien a également lancé de nombreuses cyberattaques contre l'Iran.

Mon pays est depuis longtemps la principale cible et la principale victime de cyberattaques dirigées contre ses infrastructures vitales, attaques qui perturbent la prestation des services publics et le fonctionnement de l'Administration. Les attaques de Stuxnet contre les installations nucléaires pacifiques de l'Iran, ainsi que les récentes attaques contre les infrastructures industrielles, telles que les industries sidérurgique et pétrochimique, les stations-service et les systèmes de services publics municipaux, ne sont que quelques exemples de ces cyberattaques. Le régime israélien a admis à plusieurs reprises être impliqué dans ces actes, qui sont illicites au regard du droit international, perpétrés à la faveur des technologies de l'information et des communications, avec le soutien indéfectible des États-Unis. Nous condamnons toutes ces attaques et demandons instamment à la communauté internationale de mettre les auteurs de ces attaques face à leurs responsabilités.

Malheureusement, l'Iran a récemment fait l'objet d'accusations fausses et injustifiées concernant une prétendue cyberattaque. Nous rejetons toute allégation fictive formulée contre nous, et qui repose sur des allégations fabriquées de toutes pièces et des conceptions erronées formulées à notre endroit à des fins politiques. Étant donné la nature et les caractéristiques techniques du cyberespace et la difficulté de déterminer les responsabilités dans l'environnement numérique, l'Iran signale qu'imputer des responsabilités à des États de façon indue et sous de faux prétextes comporte des conséquences délétères. Si le Royaume-Uni était réellement préoccupé par les effets potentiels sur la sécurité, l'économie, la société et les conditions humanitaires, il s'abstiendrait de faire des déclarations hâtives susceptibles de répandre de fausses informations.

En conclusion, pour la République islamique d'Iran, le meilleur moyen de garantir un environnement numérique sûr et sécurisé est d'élaborer de nouvelles normes et règles juridiques internationales concernant la prévention de l'utilisation des TIC et du cyberespace à des fins malveillantes, ainsi que le règlement pacifique des différends, dans le cadre d'un instrument juridiquement contraignant.

Le Président (*parle en anglais*) : Je donne maintenant la parole à l'Observateur du Saint-Siège.

Mgr Caccia (Saint-Siège) (*parle en anglais*) : Dans sa lettre encyclique *Fratelli Tutti*, le pape François a écrit que le nombre toujours croissant d'interconnexions et de communications qui enveloppent notre planète rend plus palpable la conscience de l'unité et du partage d'un destin commun entre les nations. Toutefois, cette unité est menacée par l'utilisation malveillante croissante des technologies de l'information et des communications (TIC) par des acteurs étatiques et non étatiques. Cette utilisation malveillante des TIC découle partiellement du fait que notre immense progrès technologique n'a pas été accompagné d'un développement de l'être humain en responsabilité, en valeurs, en conscience. À cet égard, le Saint-Siège se félicite de la convocation du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, qui offre une bonne occasion de corriger ce déséquilibre. Ma délégation a suivi ces réunions avec un grand intérêt et, à l'avenir, continuera de prendre une part active à ses travaux. Le réseau de systèmes interconnectés qui constitue le cyberespace constitue un environnement partagé, dont le maintien exige que nous passions tous du paradigme de la concurrence à celui de la coopération. Un tel changement nécessite un ensemble de principes communs. Dans cet esprit, ma délégation voudrait vous faire part de quelques considérations.

Premièrement, le comportement des États dans le cyberespace doit respecter la dignité inhérente à chaque personne humaine. À cette fin, les États doivent promouvoir et protéger la liberté d'expression en ligne de chaque personne. Cette liberté, indispensable à la recherche de la vérité, a aussi ses limites, liées à l'ordre moral et à l'intérêt général. Le respect de la dignité humaine dans le cyberespace oblige les États à respecter également le droit à la vie privée en protégeant les citoyens d'une

surveillance intrusive et en leur permettant de protéger leurs informations personnelles d'un accès non autorisé.

Deuxièmement, les États doivent veiller à ce que les personnes qui se trouvent dans la situation la plus vulnérable soient protégées contre les préjudices. Cela signifie qu'il faut non seulement protéger ses propres infrastructures critiques, telles que les hôpitaux, les systèmes d'approvisionnement en eau, les centrales électriques et les installations qui contiennent des forces dangereuses, mais aussi s'abstenir de toute activité visant à endommager intentionnellement les infrastructures critiques d'un autre État.

Troisièmement, les États doivent être guidés par la justice dans leurs actions dans le cyberespace, ce qui implique que les États en mesure de le faire contribuent effectivement aux efforts visant à réduire la fracture numérique. Non seulement cette fracture conduit à des modèles inégaux de développement humain, mais elle crée également des cybervulnérabilités qui menacent tous les pays. Pour remédier à ces vulnérabilités, le Saint-Siège préconise des efforts de renforcement des capacités au profit des États qui ne bénéficient pas d'une part égale des fruits de la révolution numérique. Ce renforcement des capacités doit rester politiquement neutre et sans conditions.

L'humanité est entrée dans une nouvelle ère où nos prouesses techniques nous ont amenés à un carrefour qui nous offre à la fois de grandes promesses et de grands risques. Pour que les nouvelles avancées dans le domaine des TIC contribuent au développement humain intégral, nous devons évaluer en permanence la manière dont les nouveaux outils peuvent être appliqués dans le respect de la dignité humaine. Ma délégation espère que ces efforts ainsi que la poursuite de l'élaboration, par le groupe de travail à composition non limitée, des normes de comportement responsable des États nous permettront de nous réjouir de ces progrès et de nous enthousiasmer pour les immenses possibilités qu'ils continuent d'ouvrir devant nous.

Le Président (*parle en anglais*) : La Commission vient d'entendre le dernier orateur sur le groupe de questions « Autres mesures de désarmement et sécurité internationale ».

Je vais maintenant donner la parole aux délégations qui ont demandé à exercer leur droit de réponse. À cet égard, je rappelle aux délégations les limites de temps et leur demande d'en être conscientes.

M. Shin (Fédération de Russie) (*parle en russe*) : Je voudrais exercer mon droit de réponse concernant le discours hostile contenu dans certaines des déclarations que nous avons entendues aujourd'hui.

Je dois avouer que j'ai été assez troublé par les déclarations des représentants des États-Unis, de l'Union européenne, du Royaume-Uni, de l'Australie et d'un certain nombre d'autres États, qui ont affirmé leur soutien au groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et ont évoqué les aspects positifs de ce mécanisme. Je me souviens très bien que ce sont ces mêmes pays qui ont voté contre la création du groupe de travail à composition non limitée – et pas seulement une fois, mais deux. Cela signifie-t-il qu'ils ne disent plus la vérité aujourd'hui ? Pourquoi devrions-nous croire ce qu'ils disent ou font ? Aujourd'hui, ils promeuvent avec assurance le projet de résolution A/C.1/77/L.73, relatif à un programme d'action sur les questions liées à la cybernétique, en affirmant qu'ils le font dans l'intérêt du groupe de travail à composition non limitée. Je voudrais leur demander de préciser de quoi ils parlent exactement. Plus nous entendons parler du programme d'action, plus nous nous posons de questions.

Nous ne comprenons pas pourquoi il est demandé aux États Membres de l'ONU de créer d'abord ce cadre et de décider ensuite de ce qu'il va réellement faire, y compris le mécanisme de prise de décisions et le financement de ce processus. On nous demande en fait de mettre la charrue avant les bœufs. Pourquoi ne pas discuter d'abord de cette initiative dans le cadre du groupe de travail à composition non limitée, dans le plein respect de son mandat et des accords consensuels antérieurs ? Nous pensons qu'une période de trois ans, jusqu'en 2025, est plus que suffisante pour développer conjointement une compréhension de la faisabilité de la création d'un tel cadre ainsi que de sa portée et de ses modalités potentielles.

Franchement, les actions de la France et de ses partenaires ressemblent à une tentative de créer un mécanisme qui ne conviendrait qu'à quelques-uns, principalement les États occidentaux. Dans ce contexte, ils prendraient des décisions et les imposeraient ensuite à la grande majorité des États. Dès lors, cette initiative s'apparente à un manifeste de cybercolonialisme. La décision de faire participer des entités non étatiques aux travaux du groupe de travail à composition non limitée relève, comme nous le savons tous, du droit souverain des États.

Les demandes de nombreuses organisations russes ont également été rejetées sans explication. À notre avis, avant de parler de permettre aux organisations non gouvernementales de participer aux processus de négociation interétatiques, il faudrait d'abord assurer l'accès sans entrave des États et de leurs délégations nationales à la tribune de l'ONU. À cet égard, nous tenons à protester vigoureusement contre les actions du Gouvernement des

États-Unis qui, en utilisant les visas comme une arme, viole systématiquement les obligations que lui impose son statut d'État hôte du Siège de l'Organisation des Nations Unies.

Nous continuons d'entendre des accusations absolument infondées contre la Russie en matière de cyberagression, y compris dans le contexte de l'opération militaire spéciale en Ukraine. Au lieu d'utiliser les canaux de communication établis des organismes compétents, nos collègues occidentaux ont pris l'habitude de s'en prendre à certains États qu'ils n'apprécient pas sur la base d'affirmations sans fondement, détournant ainsi l'attention de l'opinion publique mondiale de leurs propres actions. L'objectif de leur discours est de dissimuler une campagne de cyberagression sans précédent engagée contre la Russie et d'autres États. De nombreux éléments montrent que les services de renseignement des États-Unis et des pays de l'OTAN ont mené des activités systématiques et agressives dans le cyberespace. Je rappelle les révélations d'Edward Snowden et, comme autre exemple, le récent rapport publié par nos collègues chinois sur les cyberattaques visant l'Université polytechnique du Nord-Ouest, qui ont été menées avec la participation directe de l'Agence nationale de sécurité des États-Unis. Ils ne cachent pas leurs efforts pour pratiquer la cyberguerre et mener des exercices, invitant des représentants extérieurs à leur bloc à y participer. Par ailleurs, le commandant de l'United States Cyber Command, Paul Nakasone, a publiquement reconnu que son pays menait des cyberopérations offensives contre la Russie, notamment en utilisant principalement l'armée informatique de l'Ukraine, créée par les Américains eux-mêmes.

Depuis le début de l'année, le nombre d'attaques visant les ressources des réseaux russes a plus que quadruplé par rapport à la même période l'année dernière. La plupart de ces attaques proviennent des États-Unis ou des pays de l'Union européenne. L'ampleur de la cyberagression montre qu'elle est menée de manière coordonnée par les Gouvernements des pays occidentaux, en coopération avec des communautés de pirates informatiques et des entreprises privées. Malheureusement, je n'ai pas assez de temps pour entrer dans les détails de ce sujet, mais il importe de comprendre qu'une escalade des tensions dans le cyberespace n'est pas dans l'intérêt de la communauté internationale, qui est mieux servi par la prévention des conflits et l'utilisation des technologies de l'information et des communications à des fins pacifiques et de développement.

M. Kim Song (République populaire démocratique de Corée) (*parle en anglais*) : Ma délégation se sent obligée de prendre la parole pour exercer son droit de réponse en réaction à la remarque imprudente formulée par la représentante du Royaume-Uni.

Nous rejetons catégoriquement les allégations sans fondement formulées par le Royaume-Uni à l'endroit de la République populaire démocratique de Corée. Nous connaissons bien la mauvaise habitude du Royaume-Uni d'accuser de manière inconsidérée autrui sans aucune preuve précise. D'autre part, le Royaume-Uni participe activement à différents types d'actes malveillants dans le cyberespace par le biais d'outils tels que les Cinq Yeux, afin de s'ingérer dans les affaires intérieures d'États souverains. L'allégation du Royaume-Uni revient à ce qu'un coupable intente en premier une action en justice.

Nous n'attendons rien d'autre du Royaume-Uni, qui suit aveuglément les traces de la politique hostile des États-Unis à l'égard de la République populaire démocratique de Corée, dans le but de diaboliser notre pays sur la scène internationale et d'imposer une prétendue coopération internationale pour faire pression sur la République populaire démocratique de Corée. L'allégation infondée soulevée par le Royaume-Uni révèle clairement ses préjugés et son hostilité extrêmes à l'égard de la République populaire démocratique de Corée. Nous demandons instamment au Royaume-Uni de reprendre ses esprits et de réfléchir à son comportement imprudent et scandaleux.

M. Li Song (Chine) (*parle en chinois*) : La Chine prend note des accusations sans fondement lancées par la représentante du Royaume-Uni contre les cyberactivités de la Chine et les rejette fermement.

La Chine s'est fermement engagée à préserver la cybersécurité. Elle est également une victime majeure des cyberattaques. Le Gouvernement chinois s'oppose fermement à toutes les formes de cyberattaques et les combat conformément à la loi, ce qui démontre pleinement son attitude responsable dans le domaine de la cybersécurité.

La Chine tient à souligner que la cybersécurité est une menace qui pèse sur tous les pays. Tous les pays devraient, sur la base du respect mutuel, de l'égalité et des avantages réciproques, privilégier le dialogue et la coopération pour répondre conjointement aux menaces qui pèsent sur la cybersécurité. Nous demandons instamment aux pays concernés de cesser de calomnier la Chine et de l'accuser sans fondement de cyberattaques, et d'adopter effectivement une attitude responsable, en collaborant avec toutes les parties pour préserver la paix et la sécurité dans le cyberespace.

M. Bourgel (Israël) (*parle en anglais*) : Je me vois contraint de prendre la parole suite aux références faites concernant mon pays par le représentant de la République islamique d'Iran. Israël rejette ces allégations malveillantes.

Compte tenu du comportement de l'Iran dans le domaine cybernétique, et en particulier dernièrement avec la dangereuse cyberattaque contre les infrastructures de l'Albanie, ses remarques ne sont rien moins qu'absurdes.

À cet égard, je tiens également à condamner les deux récentes cyberattaques contre des opérations de maintien de la paix des Nations Unies, qui ont toutes deux été menées par le régime iranien et ses supplétifs. Comme c'est le cas pour tant des questions examinées à la Commission, l'Iran agit systématiquement contre la communauté internationale pour provoquer l'effondrement des instances de maîtrise des armements. Tout comme l'Iran parraine et soutient des groupes terroristes afin de susciter la peur parmi les États de la région, il tente d'utiliser des outils malveillants dans le domaine des technologies de l'information et des communications afin de susciter la peur et la destruction parmi les États du monde entier.

M^me^ McIntyre (France) : Je souhaite exercer le droit de réponse de mon pays en réponse aux propos tenus par la délégation de la Fédération de Russie concernant notre projet de résolution A/C.1/77/L.73, intitulé « Programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale ».

Comme les membres le savent, la France a proposé, de manière transparente et ouverte, à l'ensemble des États Membres de l'ONU, un projet de résolution visant à créer un programme d'action en matière de renforcement des capacités dans le domaine cyber. Ce projet a été discuté longuement et ouvertement au cours de quatre réunions de consultations ouvertes, qui se sont tenues ici à New York, ainsi qu'à Genève préalablement. Le projet a été considérablement amélioré pour tenir compte des nombreuses propositions qui ont été faites par les délégations, et je les en remercie.

Ce projet s'inspire des consultations qui ont déjà été tenues pour créer le Programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous tous ses aspects. Je rappelle la séquence qui avait été observée : un rapport du Secrétaire général en premier lieu, puis deux années de consultations visant à tenir compte de l'ensemble des suggestions des États Membres de l'ONU pour le contenu de ce programme d'action et, enfin, l'adoption du programme d'action par une conférence internationale, en bout de course. C'est précisément la séquence que nous avons proposée dans notre projet de résolution A/C.1/77/L.73, en confiant le soin au Secrétaire général de présenter, dès l'année prochaine, un rapport visant à préciser les modalités et le contenu de ce futur programme d'action, tout en respectant pleinement les prérogatives du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), qui devra, bien sûr, discuter également des modalités de ce programme d'action, tout en laissant le soin aux États Membres, ensuite, s'ils le souhaitent, de procéder à son adoption.

Notre processus, je le rappelle, est donc ouvert, transparent et inclusif, et il vise à respecter l'ensemble du processus qui a décidé par les États Membres, y compris au sein du groupe de travail à composition non limitée, et nous continuerons à adopter cette approche transparente et inclusive jusqu'à la fin des discussions.

M. Balouji (République islamique d'Iran) (*parle en anglais*) : Je me vois contraint de prendre la parole pour réfuter les allégations faites par le représentant israélien contre mon pays.

Nous ne sommes pas surpris que les mensonges prolifèrent dans les déclarations du représentant de ce régime qui n'a aucun respect pour le droit international. Il n'a cessé de lancer des cyberattaques contre de nombreux secteurs en Iran, des installations nucléaires pacifiques aux services publics tels que l'aide d'urgence. Nous sommes bien conscients que le régime israélien est un régime oppressif et d'apartheid, et nous connaissons son sombre bilan en matière de droits de l'homme et son mépris pour les appels internationaux à adhérer au Traité sur la non-prolifération des armes nucléaires, à la Convention sur les armes chimiques et à la Convention sur les armes biologiques, entre autres.

Israël a violé 29 résolutions du Conseil de sécurité, qui sont juridiquement contraignantes pour les États Membres en vertu de l'Article 25 de la Charte des Nations Unies, notamment les résolutions 54 (1948), 111 (1956), 233 (1967), 234 (1967), 236 (1967), 248 (1968), 250 (1968), 252 (1968), 256 (1968), 262 (1968), 267 (1969), 270 (1969), 280 (1970), 285 (1970), 298 (1971), 313 (1972), 316 (1972), 468 (1980), 476 (1980) et, surtout, la résolution 2231 (2015), ne ratant aucune occasion et n'épargnant aucun effort pour qu'elle demeure lettre morte. Un tel régime n'a aucun fondement moral pour parler de respect des règles et d'attachement au droit international.

En matière de cybersécurité, la situation est encore pire. Ce que nous avons dit n'a rien d'une allégation, puisque tous les observateurs internationaux ont confirmé les actions irresponsables d'Israël, que nous condamnons fermement.

Le Président (*parle en anglais*) : Nous avons entendu le dernier orateur au titre de l'exercice du droit de réponse.

Nous avons un peu de temps devant nous, alors essayons d'utiliser au mieux ces quelques minutes pour entamer l'examen du groupe de questions « Désarmement et sécurité sur le plan régional ». Nous avons une longue liste d'orateurs et d'oratrices pour ce groupe de questions, et j'en appelle donc à la pleine coopération des délégations.

M^me^ Kristanti (Indonésie) (*parle en anglais*) : J'ai l'honneur de prendre la parole au nom du Mouvement des pays non alignés.

Le Mouvement des pays non alignés réaffirme sa vive préoccupation face au recours croissant à l'unilatéralisme et, à cet égard, souligne que le multilatéralisme et les solutions convenues dans un cadre multilatéral, conformément à la Charte des Nations Unies, sont la seule méthode viable pour traiter les questions de désarmement et de sécurité internationale. Le Mouvement souligne également sa position de principe concernant le non-recours à la menace ou à l'emploi de la force contre l'intégrité territoriale d'un quelconque État.

Les États du Mouvement des pays non alignés qui sont parties au Traité sur la non-prolifération des armes nucléaires (TNP) sont profondément préoccupés par les doctrines de défense stratégique des États dotés d'armes nucléaires et de certains États non dotés d'armes nucléaires qui souscrivent aux garanties de sécurité nucléaire étendues fournies par les États dotés d'armes nucléaires. Ces doctrines ne se contentent pas d'énoncer des arguments motivant la menace ou l'emploi d'armes nucléaires mais perpétuent également des concepts de sécurité internationale injustifiables, fondés sur la promotion et la constitution d'alliances militaires et sur l'élaboration de politiques de dissuasion nucléaire. Le Mouvement des pays non alignés exhorte donc les États concernés à bannir totalement de leurs doctrines militaires et de sécurité la menace ou l'emploi d'armes nucléaire.

Le Mouvement réaffirme son plein soutien à la création au Moyen-Orient d'une zone exempte d'armes nucléaires et d'autres armes de destruction massive. Comme étape prioritaire à cette fin, le Mouvement des pays non alignés réaffirme qu'il faut créer rapidement au Moyen-Orient une zone exempte d'armes nucléaires, conformément à la résolution 487 (1981) et au paragraphe 14 de la résolution 687 (1991) du Conseil de sécurité, ainsi qu'aux résolutions pertinentes que l'Assemblée générale a adoptées. Le Mouvement des pays non alignés appelle toutes les parties concernées à prendre d'urgence des mesures concrètes de mise en œuvre de la proposition lancée par l'Iran en 1974 en vue de la création d'une telle zone.

Les États membres du Mouvement des pays non alignés qui sont parties au TNP se déclarent une nouvelle fois profondément déçus par le fait que le Plan d'action de 2010 sur la création au Moyen-Orient d'une zone exempte d'armes nucléaires et de toutes autres armes de destruction massive n'ait pas été mis en œuvre. Ils rejettent fermement les arguments concernant les obstacles à la mise en œuvre du Plan d'action et de la résolution de 1995 sur le Moyen-Orient. Le Mouvement insiste à nouveau sur la responsabilité particulière qui incombe aux coauteurs de la résolution de 1995 sur le Moyen-Orient en ce qui concerne sa mise en œuvre. Le Mouvement des pays non alignés note avec préoccupation que la résolution de 1995 n'a toujours pas été mise en œuvre, malgré les décisions prises lors des conférences d'examen du TNP, ce qui compromet l'efficacité et la crédibilité du TNP et perturbe l'équilibre délicat entre ses trois piliers.

À cet égard, le Mouvement des pays non alignés se félicite de la tenue de la première session de la Conférence sur la création au Moyen-Orient d'une zone exempte d'armes nucléaires et d'autres armes de destruction massive, conformément à la décision 73/546, sous la présidence du Royaume hachémite de Jordanie, et de l'adoption d'une déclaration politique par la Conférence. Le Mouvement se félicite également de la convocation de la deuxième session de la Conférence, présidée par l'État du Koweït, et de ses résultats, notamment l'adoption du règlement intérieur et la création d'un comité de travail informel. En outre, le Mouvement attend avec intérêt la troisième session de la Conférence et continue de demander à tous les États de la région, sans exception, de participer activement à la Conférence, de négocier de bonne foi et de conclure un traité juridiquement contraignant portant création d'une telle zone.

Le Mouvement estime que les zones exemptes d'armes nucléaires créées par les Traités de Tlatelolco, de Rarotonga, de Bangkok et de Pelindaba, le Traité portant création d'une zone exempte d'armes nucléaires en Asie centrale et le statut de la Mongolie comme territoire exempt d'armes nucléaires, constituent des avancées concrètes et des mesures importantes visant à renforcer le désarmement et la non-prolifération nucléaires à l'échelle mondiale. Dans le contexte des zones exemptes d'armes nucléaires, il est essentiel que les États dotés d'armes nucléaires fournissent des garanties inconditionnelles contre la menace ou l'emploi d'armes nucléaires à tous les États de ces zones, en toutes circonstances. Le Mouvement des pays non alignés exhorte tous les États dotés d'armes nucléaires à ratifier les protocoles à tous les traités portant création de zones exemptes d'armes

nucléaires, à retirer toutes leurs réserves ou déclarations interprétatives qui seraient incompatibles avec l'objet et le but de ces instruments, et à respecter le statut dénucléarisé de ces zones. Le Mouvement des pays non alignés exhorte les États à créer de nouvelles zones exemptes d'armes nucléaires, sur la base d'accords librement conclus entre les États des régions où ces zones n'existent pas.

Pour terminer, le Mouvement des pays non alignés souligne l'importance des activités que l'Organisation des Nations Unies mène à l'échelon régional pour renforcer la stabilité et la sécurité de ses États Membres, et qui peuvent être concrètement promues grâce au maintien et à la revitalisation des trois centres régionaux pour la paix et le désarmement.

M. Fuller (Belize) (*parle en anglais*) : J'ai l'honneur de prendre la parole au nom des 14 États membres de la Communauté des Caraïbes (CARICOM) sur le groupe de questions « Désarmement et sécurité sur le plan régional ».

Les États membres de la CARICOM ont adopté une approche pragmatique fondée sur la coopération et la coordination aux niveaux régional et sous-régional pour faire face aux diverses menaces qui pèsent sur la sécurité de la région. La CARICOM est pleinement engagée à jouer le rôle qui lui revient dans les efforts mondiaux visant à maintenir notre sécurité collective en mettant en œuvre nos obligations internationales. Des efforts sérieux en faveur du désarmement régional complètent nos efforts au niveau mondial.

La sécurité est un pilier essentiel de notre intégration régionale. La CARICOM a mis en place un cadre institutionnel régional pour soutenir la coopération régionale, comprenant l'Organisme d'exécution des mesures de sécurité et de lutte contre la criminalité de la CARICOM, supervisé par le Conseil des ministres chargés de la sécurité et de l'application de la loi, et complété par d'autres institutions régionales, notamment le système de sécurité régional.

Les flux illicites d'armes à feu et de munitions dans la région restent un défi majeur et sont considérés comme une menace de niveau 1 dans la stratégie de sécurité régionale de la CARICOM. Sur 10 homicides dans la région, sept sont commis à l'aide d'armes légères et de petit calibre. On estime que plus d'un demi-million d'armes à feu illégales sont en circulation rien qu'en Haïti. Les armes à feu illégales jouent un rôle clef dans tous les aspects de la criminalité transnationale organisée et facilitent les comportements criminels et déviants. Elles ont donc des conséquences socioéconomiques et un coût humain considérables.

Aucun État membre de la CARICOM n'est fabricant ou importateur majeur d'armes à feu. C'est une priorité pour la région de perturber et d'empêcher le passage d'armes à feu et de munitions illégales à nos frontières. Malgré le grand nombre d'initiatives et de mécanismes visant à résoudre les problèmes liés à la violence armée, les crimes commis à l'aide d'armes à feu restent très répandus dans la région.

La stratégie en matière de criminalité et de sécurité de la CARICOM souligne que si la région respecte le droit des autres États d'adopter des politiques libérales en matière d'accès aux armes à feu, les effets négatifs de ces politiques ne se limitent pas à leurs frontières. Elles ont des conséquences très graves pour d'autres pays, y compris les États membres de la CARICOM. La prévention du commerce illicite d'armes à feu est donc une responsabilité qui doit être partagée non seulement par les États de la CARICOM, mais aussi par les pays d'où proviennent ces armes. Lors de leur quarante-troisième réunion ordinaire, qui s'est tenue au Suriname le 3 juillet 2022, nos chefs de gouvernement ont exprimé leur inquiétude face à l'afflux d'armes à feu en provenance de l'extérieur de la région.

En 2020, les dirigeants de la CARICOM ont adopté un plan d'action pour l'exécution durable des mesures prioritaires contre la prolifération illicite des armes à feu et des munitions dans les Caraïbes à l'horizon 2030 (plan d'action des Caraïbes sur les armes à feu). L'Organisme d'exécution des mesures de sécurité et de lutte contre la criminalité prend plusieurs mesures concrètes pour mettre en œuvre ce plan d'action, notamment la fourniture d'une assistance technique et consultative aux autorités nationales, le renforcement des capacités et la formation, l'échange d'informations et de renseignements, le contrôle des frontières et des douanes, le soutien législatif par l'élaboration de lois types, la fourniture d'outils opérationnels et l'élaboration de cadres réglementaires, de politiques et de normes aux niveaux international, régional et national.

Nous voudrions attirer l'attention sur les travaux menés par l'Organisme d'exécution des mesures de sécurité et de lutte contre la criminalité dans la région, avec le soutien des gouvernements et organisations partenaires, notamment l'élaboration d'une étude complète, fondée sur des données probantes, du trafic d'armes illicites vers et dans les Caraïbes et des coûts socioéconomiques de ce trafic, en collaboration avec Small Arms Survey (SAS) ; la création d'une cellule de renseignement sur

les armes utilisées dans la criminalité (Crime Gun Intelligence Unit) de la CARICOM pour aider les États membres de la CARICOM à enquêter sur les crimes liés aux armes à feu et en poursuivre les auteurs, qui sera soutenue par des agences du Gouvernement américain telles que le Bureau of Alcohol, Tobacco, Firearms and Explosives, Homeland Security Investigations et le Bureau des douanes et de la protection des frontières ; la fourniture d'une assistance aux États membres de la CARICOM en matière de gestion d'armes à feu et de munitions ; l'établissement de partenariats importants avec de nombreux organismes internationaux afin de contribuer à la lutte contre la criminalité liée aux armes à feu, notamment INTERPOL, l'Organisation mondiale des douanes (OMD), l'Office des Nations Unies contre la drogue et le crime, le Centre régional des Nations Unies pour la paix, le désarmement et le développement en Amérique latine et dans les Caraïbes, SAS et le Mines Advisory Group ; des opérations conjointes menées du 24 au 30 septembre 2022 avec INTERPOL relatives aux armes à feu, qui ont permis de saisir quelque 320 armes, 3 300 munitions et des quantités record de drogue dans l'ensemble des Caraïbes ; des programmes de formation et de renforcement des capacités à l'intention des institutions chargées de l'application de la loi et de la sécurité, y compris les institutions douanières, en partenariat avec l'OMD ; l'appui aux États membres dans l'utilisation du Réseau régional intégré d'information balistique ; l'amélioration et l'extension du système de renseignements préalables concernant les voyageurs de la CARICOM, qui est le seul système multilatéral au monde permettant aux États de vérifier efficacement l'identité des personnes d'intérêt à bord d'un avion ou d'un navire à chaque point d'entrée dans les États participants, afin de garantir la participation de tous les États membres de la CARICOM et des États tiers intéressés à ces efforts ; la mise en place d'un système régional d'informations anticipées sur les marchandises afin d'aider les États membres de la CARICOM participants à mieux cibler certains frets ; et l'élaboration d'une loi type sur le Traité sur le commerce des armes.

Le Centre régional des Nations Unies pour la paix, le désarmement et le développement en Amérique latine et dans les Caraïbes continue d'être un partenaire important de la CARICOM. Le Centre régional est coresponsable, avec l'Organisme d'exécution des mesures de sécurité et de lutte contre la criminalité, de la mise en œuvre du plan d'action des Caraïbes sur les armes à feu. Le Centre régional des Nations Unies pour la paix, le désarmement et le développement en Amérique latine et dans les Caraïbes a mené 54 activités dans la région pour contribuer à la mise en œuvre du plan d'action, auxquelles ont participé 600 fonctionnaires, dont 220 femmes. Le Centre a également contribué à l'élaboration de guides nationaux pour la mise en œuvre du plan d'action, ainsi que pour le suivi et l'évaluation de l'état d'avancement de la mise en œuvre. À ce jour, 10 États des Caraïbes ont élaboré leur guide national.

La région a également bénéficié d'un certain nombre de webinaires et de sessions de formation sur divers sujets, notamment les meilleures pratiques internationales à l'intention des enquêteurs spécialisés dans les affaires pénales, l'examen criminalistique d'armes à feu de fabrication privée, les techniques d'enquête améliorées sur les armes à feu et la gestion des renseignements balistiques.

La CARICOM se joint à l'appel lancé par le Secrétaire général aux États Membres et aux autres partenaires pour qu'ils apportent un soutien financier et en nature au Centre.

La CARICOM considère que le Traité sur le commerce des armes, le Programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous tous ses aspects, l'Instrument international de traçage et les autres résolutions des Nations Unies relatives aux armes légères et de petit calibre sont des instruments essentiels pour prévenir, contrôler et éliminer le commerce illicite des armes légères et de petit calibre et des munitions qui y sont associées sous tous ses aspects. La CARICOM encourage tous les États à mettre pleinement en œuvre les dispositions de ces instruments.

L'un des principaux défis auxquels sont confrontés les petits États insulaires en développement dans l'application des instruments relatifs aux armes légères et de petit calibre est le manque de ressources et de capacités techniques adéquates. Pour une application complète et efficace du Traité sur le commerce des armes, du Programme d'action et de l'Instrument international de traçage, la coopération et l'assistance internationales devraient être considérées comme un partenariat entre les États en développement, les États développés et les États donateurs, ancré dans l'appropriation nationale. Nous soulignons donc qu'il importe de fournir une assistance inconditionnelle et non discriminatoire aux pays en développement, à leur demande, afin de renforcer leur capacité de mettre effectivement en œuvre les dispositions des instruments internationaux en matière de désarmement.

L'une des principales difficultés auxquelles se heurtent les États en développement, y compris la CARICOM, pour appliquer le Traité sur le commerce des armes, le Programme d'action et l'Instrument international de traçage est l'absence de transfert de technologie et de

partage des enseignements tirés de l'expérience en ce qui concerne leur mise en œuvre. Il est indispensable de redoubler d'efforts pour remédier à ce déséquilibre afin de pouvoir renforcer la maîtrise des armes légères et de petit calibre et réduire la fracture numérique technologique entre les pays développés et les pays en développement.

Consciente que la cybersécurité fait désormais partie intégrante de la sécurité régionale et que, si elle n'est pas abordée de toute urgence, elle pourrait gravement entraver le développement socioéconomique des États des Caraïbes, la région a élaboré un plan d'action de la CARICOM en matière de cybersécurité et de cybercriminalité. Le plan vise à remédier aux vulnérabilités de chaque pays participant des Caraïbes en matière de cybersécurité et à établir une norme concrète et harmonisée de pratiques, systèmes et compétences en matière de cybersécurité à laquelle chaque pays des Caraïbes pourrait aspirer à court et moyen terme. Ce plan cherche également à renforcer les capacités et infrastructures nécessaires pour permettre de détecter rapidement la cybercriminalité et les liens possibles avec les autres formes d'activités criminelles, de mener les enquêtes et d'engager les poursuites dans les meilleurs délais.

Bien que notre région dispose de ressources limitées pour faire face aux divers défis complexes en matière de sécurité résultant de frontières poreuses, de limites maritimes et terrestres étendues et d'une situation géographique en zone de transit, nous avons mis en place un certain nombre de partenariats pour concrétiser le désarmement régional par le biais d'un certain nombre de mesures pratiques.

Le Président (*parle en anglais*) : Nous sommes arrivés au terme du temps qui nous est imparti. La Commission se réunira à nouveau demain matin et entendra tout d'abord un exposé du Président du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation. Ensuite, nous poursuivrons le débat sur le groupe de questions « Désarmement et sécurité sur le plan régional ».

Je rappelle aux membres que, demain, à l'issue de sa séance du matin, la Commission tiendra sa traditionnelle cérémonie de remise des diplômes aux lauréats du Programme de bourses d'études des Nations Unies sur le désarmement.

La séance est levée à 18 h 5.