Nations Unies A/C.1/78/PV.20

Assemblée générale

Soixante-dix-huitième session

Documents officiels

Première Commission

20e séance plénière

Mardi 24 octobre 2023, à 10 heures

New York

Président : M. Paulauskas . . . . . (Lituanie)

La séance est ouverte à 10 h 5.

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 Commission va maintenant reprendre le débat thématique sur le groupe de questions « Armes classiques ». Avant de donner la parole aux délégations, je rappelle de nouveau que toutes les délégations doivent s'efforcer de respecter le temps de parole fixé pour le débat thématique.

Je donne la parole à l'Observateur du Saint-Siège.

Mgr Caccia (Saint-Siège) (*parle en anglais*) : Tout d'abord, ma délégation rappelle que tous les États parties au Traité sur la non-prolifération des armes nucléaires ont pour obligation commune de « poursuivre de bonne foi des négociations [...] sur un traité de désarmement général et complet ». Il est devenu encore plus impératif de réaffirmer cet objectif dans le contexte de la prolifération rapide des armes à l'échelle mondiale.

Plus inquiétant encore, la guerre en Ukraine se caractérise par l'utilisation généralisée d'armes aveugles, à savoir les mines antipersonnel et les armes à sous-munitions. Le Saint-Siège appelle à la cessation immédiate de l'utilisation de ces armes, qui mettent en danger les civils, en particulier les enfants, et contaminent notre planète. Comme l'a souligné le pape François, les préoccupations morales que suscite la guerre nucléaire ne doivent pas reléguer au second plan les problèmes éthiques de plus en plus urgents que soulève l'utilisation, dans les guerres contemporaines, d'armes dites classiques, qui ne doivent être utilisées qu'à des fins défensives et ne pas viser des cibles civiles. En effet, la dévastation que laissent dans leur sillage les armes classiques appelle à prendre de nouvelles mesures propres à limiter la propagation de ces armes, à accroître la transparence en ce qui concerne les stocks d'armes existants et à garantir que tout emploi soit conforme au droit international humanitaire.

Dans le cadre de cette entreprise, la communauté internationale doit toujours accorder une place primordiale à la dignité intrinsèque de l'être humain. À cet égard, le Saint-Siège renouvelle son appui au Programme d'action des Nations Unies en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous tous ses aspects, dans lequel les États se sont déclarés déterminés à « renforcer le respect de la vie », et espère que de nouvelles avancées seront faites en ce qui concerne le programme de la quatrième Conférence des Nations Unies chargée d'examiner les progrès accomplis dans l'exécution du Programme d'action, qui se tiendra l'année prochaine. De même, ma délégation appuie l'appel lancé par le Secrétaire général en faveur de négociations en vue d'adopter, d'ici à 2026, un instrument juridiquement contraignant visant à interdire les

systèmes d'armes létaux autonomes qui fonctionnent sans contrôle ou surveillance humaine. Dans l'intervalle, le Saint-Siège exhorte tous les États à s'abstenir de mettre au point de telles armes, qui ne pourront jamais être des sujets moralement responsables et bafouent les exigences de la conscience publique.

Les conflits armés se déroulant de plus en plus souvent dans des villes et agglomérations densément peuplées, l'utilisation d'armes explosives s'avère souvent aveugle, ce qui donne lieu à des pertes inacceptables parmi les non-combattants et à la destruction d'infrastructures indispensables à la survie des populations civiles. Face à cette situation, le Saint-Siège salue l'adoption, à Dublin en novembre dernier, de la Déclaration politique sur le renforcement de la protection des civils contre les conséquences humanitaires découlant de l'utilisation d'armes explosives dans les zones peuplées. Le Saint-Siège remercie le Gouvernement irlandais de son rôle moteur dans cette entreprise et espère que la Déclaration fera passer les opérations militaires d'un paradigme de dommages collatéraux à un paradigme de protection, réduisant ainsi au minimum les pertes en vies humaines.

Pour conclure, je tiens à me faire l'écho du message du pape François relayé au Conseil de sécurité en juin :

> « [D]'un point de vue économique, la guerre est souvent plus séduisante que la paix, dans la mesure où elle favorise le profit, mais c'est toujours pour quelques-uns et au détriment du bien-être de populations entières. L'argent gagné grâce aux ventes d'armes est donc souillé par le sang d'innocents. Il faut plus de courage pour renoncer à des profits faciles au nom du maintien de la paix que pour vendre des armes toujours plus sophistiquées et plus puissantes. Il faut plus de courage pour rechercher la paix que pour faire la guerre » (*S/PV.9346, p. 6*).

Le Président (*parle en anglais*) : La Commission a entendu le dernier orateur du débat thématique sur le groupe de questions « Armes classiques ».

La Commission va maintenant entamer le débat thématique sur le groupe de questions « Autres mesures de désarmement et sécurité internationale ».

M. Sirie (Indonésie) (*parle en anglais*) : J'ai le plaisir de prendre la parole au nom du Mouvement des pays non alignés.

Le Mouvement souligne les avantages offerts par les technologies de l'information et des communications (TIC) et leur contribution au développement, et encourage les États à mettre en œuvre les normes, règles et principes de comportement responsable des États tout en poursuivant le débat sur les mécanismes de mise en œuvre, car cela contribuera à renforcer la stabilité et la sécurité du cyberespace.

Par ailleurs, le Mouvement rejette fermement l'utilisation malveillante des nouvelles TIC à des fins incompatibles avec les objectifs de maintien de la paix et de la sécurité internationales. Il appelle à intensifier les efforts déployés pour éviter que le cyberespace ne devienne le théâtre de conflits et à garantir au contraire des utilisations exclusivement pacifiques qui permettraient de réaliser pleinement le potentiel des TIC pour contribuer au développement socioéconomique des pays.

Le Mouvement prend note des conclusions que le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale a formulées dans ses rapports de 2013, 2015 et 2021, à savoir que le droit international, en particulier la Charte des Nations Unies, est applicable et essentiel au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement numérique ouvert, sûr, stable, accessible et pacifique.

Le Mouvement rappelle 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 en application de la résolution 73/27, a été le premier mécanisme inclusif mis en place dans le cadre de l'Organisation des Nations Unies avec la participation de tous les États Membres, agissant sur la base du consensus.

Le Mouvement réaffirme sa détermination à assurer le succès du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), créé en application de la résolution 75/240, qui est actuellement le seul mécanisme inclusif qui tienne compte des préoccupations et des intérêts de tous les États, repose sur un consensus et mène ses activités sous les auspices de l'ONU, avec la participation active de tous les États, dans des conditions d'égalité. Le Mouvement prend également note du processus d'adoption par consensus du deuxième rapport d'activité annuel du groupe de travail (voir A/78/265).

Le Mouvement des pays non alignés souligne que tout cadre juridique international conçu pour traiter les questions relatives aux utilisations des TIC qui pourraient avoir une incidence sur la paix et la sécurité internationales doit tenir compte des préoccupations et

des intérêts de tous les États, reposer sur un consensus et être élaboré sous les auspices de l'ONU, avec la participation active de tous les États, dans des conditions d'égalité. À cet égard, le Mouvement est favorable à un mécanisme permanent à voie unique, dirigé par les États et placé sous l'égide de l'Organisation, qui ferait rapport à la Première Commission. Il appuie la mise en place d'un processus ouvert, inclusif, transparent, durable et flexible, capable de s'adapter aux besoins des pays en développement et à l'évolution de l'environnement numérique. Le Mouvement souligne en outre qu'un tel cadre juridique, conjugué à une instance multilatérale inclusive consacrée à la coopération internationale sur la préservation de l'utilisation des TIC à des fins pacifiques, apporterait une contribution majeure au renforcement de la stabilité et de la sécurité du cyberespace en prévenant les conflits, promouvant ainsi le règlement des différends internationaux par des moyens pacifiques et les utilisations pacifiques des TIC. Dans le même temps, le Mouvement souligne sa position de principe : ce cadre juridique ne doit en rien porter atteinte au droit inaliénable des États de mettre au point et d'utiliser des TIC à des fins pacifiques.

Le Mouvement des pays non alignés rejette toute mesure unilatérale contraire à la Charte des Nations Unies et au droit international qui entrave la pleine réalisation du développement socioéconomique et le bien-être des populations des pays concernés. Il condamne l'utilisation à mauvais escient des TIC, y compris Internet et les médias sociaux, pour commettre des actes de terreur ou inciter à leur commission. Il souligne l'importance du renforcement des capacités des États Membres et des mesures de confiance visant à améliorer la stabilité et la sécurité du cyberespace.

Le Mouvement souligne également qu'il importe de respecter les normes environnementales dans l'élaboration et l'application des accords de désarmement et de limitation des armements. Il réaffirme en outre que les instances internationales consacrées au désarmement doivent tenir dûment compte des normes pertinentes relatives à l'environnement lorsqu'elles négocient des traités et accords de désarmement et de limitation des armements.

Le Mouvement des pays non alignés se félicite de l'adoption sans vote de la résolution 77/45, sur la relation entre le désarmement et le développement. Il souligne en outre l'importance de la réduction des dépenses militaires, conformément au principe d'une sécurité non diminuée au niveau d'armement le plus bas, et demande instamment à tous les États de consacrer les ressources ainsi dégagées à remédier aux nouvelles difficultés qui attendent la communauté internationale concernant le développement, l'éradication de la pauvreté et l'élimination des maladies qui affligent l'humanité.

Dans le cadre de ce groupe de questions, le Mouvement des pays non alignés a déposé trois projets de résolution, intitulés « Respect des normes environnementales dans l'élaboration et l'application des accords de désarmement et de maîtrise des armements » (A/C.1/78/L.6), « Promotion du multilatéralisme dans le domaine du désarmement et de la non-prolifération » (A/C.1/78/L.7) et « Relation entre le désarmement et le développement » (A/C.1/78/L.4), et invite tous les États Membres à les appuyer.

M. Chindawongse (Thaïlande) (*parle en anglais*) : J'ai l'honneur de faire la présente déclaration au nom de l'Association des nations de l'Asie du Sud-Est (ASEAN).

L'ASEAN s'associe à la déclaration que vient de prononcer le représentant de l'Indonésie au nom du Mouvement des pays non alignés.

L'ASEAN réaffirme sa détermination à bâtir un cyberespace ouvert, sûr, stable, accessible, interopérable, pacifique et résilient qui favorise le progrès économique, le renforcement de la connectivité régionale et l'amélioration du niveau de vie de tous. Dans le même temps, elle reconnaît l'omniprésence des cybermenaces, qui sont en constante évolution, et transfrontières par nature. Dans un contexte de numérisation généralisée de l'économie et de prolifération des appareils connectés à Internet dans l'ASEAN, nous sommes devenus de plus en plus vulnérables aux cyberactivités malveillantes qui sont susceptibles de compromettre la paix et la sécurité. À cet égard, l'ASEAN est convaincue que les États doivent œuvrer ensemble pour répondre efficacement aux cybermenaces, réduire au minimum le risque de perception erronée et d'erreur d'appréciation en développant la confiance, et exploiter les avantages de la technologie tout en reconnaissant que la cybersécurité est une question transversale qui nécessite les compétences coordonnées de multiples parties prenantes dans différents domaines.

L'ASEAN souligne le rôle central que joue l'Organisation des Nations Unies dans les débats sur la cybersécurité. À cet égard, elle réaffirme son soutien aux travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), en tant que mesure de confiance et cadre permettant de forger encore et encore le consensus sur cette question importante. Dès lors, l'ASEAN se félicite

de l'adoption par consensus du deuxième rapport d'activité annuel du groupe de travail à composition non limitée (voir A/78/265) à sa cinquième session de fond, en juillet. L'ASEAN est fière que ses initiatives, en particulier le répertoire d'interlocuteurs du Forum régional de l'ASEAN chargés de la sécurité du numérique et de son utilisation et la matrice du plan d'action régional de l'ASEAN sur la mise en œuvre de normes de comportement responsable des États dans le cyberespace, aient contribué de manière significative aux débats internationaux sur le cyberespace tenus à l'ONU. Nous attendons avec intérêt la création et la mise en service d'un répertoire mondial et intergouvernemental d'interlocuteurs, ainsi que l'élaboration de nouvelles orientations, y compris une liste de contrôle, sur la mise en œuvre des normes, comme indiqué dans le rapport d'activité annuel.

L'ASEAN plaide pour que le groupe de travail à composition non limitée demeure, jusqu'à la fin de son mandat, l'instance centrale des débats sur la cybersécurité tenus à l'Organisation, et attend avec impatience de nouveaux progrès, notamment grâce au consensus durement acquis auquel nous sommes parvenus autour des deux précédents rapports d'activité annuels. L'ASEAN appelle les États Membres à reconnaître l'importance de préserver et de maintenir le consensus sur la question majeure qu'est la cybersécurité. Nous devons également éviter de créer des processus qui se chevauchent ou des mécanismes parallèles qui ne feraient que restreindre davantage les ressources limitées de l'ONU et de ses États Membres. À cet égard, l'ASEAN est convaincue qu'il importe d'avoir en place un processus à voie unique qui s'appuie sur les recommandations consensuelles du groupe de travail à composition non limitée relatives à un dialogue institutionnel régulier. L'ASEAN reste pleinement attachée à engager un dialogue constructif avec tous les partenaires à cette fin.

Au sein de l'ASEAN, la coopération en matière de cybersécurité recoupe plusieurs piliers et secteurs, conformément au Plan directeur numérique de l'Association pour 2025 et à sa stratégie de coopération en matière de cybersécurité pour la période 2021-2025, qui ont été adoptés en janvier 2022 par les ministres des pays de l'ASEAN chargés des questions numériques. Les États membres de l'ASEAN ont fait des efforts pour mettre en œuvre des mesures de cybersécurité renforcées conformes à la stratégie pour la période 2021-2025, compte tenu de l'augmentation récente des attaques et des menaces sur la cybersécurité à l'échelle mondiale et en réponse aux derniers faits nouveaux survenus dans le domaine cybernétique. Parallèlement, l'Association travaille actuellement à l'application de son plan d'action régional sur la mise en œuvre des recommandations 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, élaboré pour permettre aux États membres de l'ASEAN de déterminer les domaines qui nécessitent un soutien supplémentaire afin de mettre en œuvre les normes de comportement responsable, y compris le renforcement des capacités et la coopération internationale.

Pour renforcer ses capacités de réaction aux cyberincidents, l'ASEAN a décidé de créer l'équipe régionale d'intervention informatique d'urgence de l'Association afin de permettre aux équipes nationales d'intervention informatique d'urgence des États membres de l'ASEAN d'échanger rapidement des informations sur les menaces et les attaques.

La cybersécurité étant une question transversale, le Comité de coordination de la cybersécurité de l'ASEAN a été créé pour renforcer la collaboration et la coordination régionales en matière de cybersécurité. Le Comité comprend des représentants des organismes sectoriels concernés afin de renforcer la coordination intersectorielle en matière de cybersécurité tout en respectant les domaines de travail des organismes sectoriels.

L'ASEAN souligne l'importance de la coopération internationale et du renforcement des capacités dans le domaine du numérique en vue de donner aux États, en particulier les pays en développement, les moyens de lutter efficacement contre les cybermenaces et de mettre en œuvre les 11 normes volontaires non contraignantes relatives à l'utilisation responsable du numérique par les États. À cette fin, l'ASEAN a entamé la mise en œuvre du projet de cyberbouclier de l'ASEAN pour la période 2023-2026 afin de compléter les efforts de renforcement des capacités déployés par l'Association, notamment le Centre d'excellence ASEAN-Singapour pour la cybersécurité, sis à Singapour, et le Centre de renforcement des capacités en cybersécurité ASEAN-Japon, situé en Thaïlande, en vue de soutenir l'objectif commun de renforcement des capacités de la région. L'ASEAN se réjouit à la perspective de collaborer avec l'ONU à cet égard, notamment dans le cadre du partenariat global ASEAN-Organisation des Nations Unies.

En outre, l'ASEAN travaille avec des partenaires internationaux pour renforcer la coopération internationale dans le domaine de la sécurité numérique, par l'intermédiaire d'instances telles que la réunion

intersessions du Forum régional de l'ASEAN sur la sécurité du numérique et de son utilisation. L'ASEAN se félicite également des progrès accomplis grâce à l'ouverture du Centre d'excellence en matière de cybersécurité et d'information de la Réunion des ministres de la défense de l'ASEAN et à la mise en place du groupe de travail d'experts sur la cybersécurité de la Réunion des ministres de la défense de l'ASEAN-Plus. Parmi les réalisations notables de ces dernières années figurent la création d'un répertoire d'interlocuteurs et de techniciens, l'élaboration d'un glossaire de la terminologie cybernétique, l'organisation d'un exercice de simulation et la mise en place du portail du groupe de travail d'experts sur la cybersécurité de la Réunion des ministres de la défense de l'ASEAN-Plus.

Pour conclure, l'ASEAN réaffirme sa détermination à se préparer pour l'avenir afin de favoriser le progrès économique, d'améliorer notre mode de vie et de garantir la paix et la sécurité pour tous. Nous attendons avec intérêt de contribuer de manière constructive, avec les membres de la communauté internationale et les parties prenantes concernées, à la promotion de notre objectif commun de parvenir à un cyberespace pacifique, sûr, interopérable et résilient.

M. Shen Jian (Chine) (*parle en anglais*) : J'ai l'honneur de faire la présente déclaration commune au nom du Bélarus, du Burundi, du Cambodge, du Cameroun, de Cuba, de la Dominique, de l'Érythrée, de l'Éthiopie, de la Gambie, de la Guinée-Bissau, de la Guinée équatoriale, du Kazakhstan, du Kirghizstan, du Nicaragua, du Pakistan, de la République démocratique populaire lao, de la Russie, de la Somalie, de la Syrie, de Vanuatu, du Venezuela, du Zimbabwe et de mon propre pays, la Chine.

À l'occasion du deuxième anniversaire de l'adoption de la résolution 76/234, intitulée « Promotion de la coopération internationale touchant les utilisations pacifiques dans le contexte de la sécurité internationale », nous, auteurs de la résolution, réaffirmons le droit inaliénable de tous les États de participer à un échange aussi complet que possible d'équipements, de matières et d'informations scientifiques et technologiques à des fins pacifiques. À l'aube d'une ère nouvelle, compte tenu des conséquences potentielles des progrès scientifiques et technologiques sur la sécurité mondiale, le rôle des utilisations pacifiques devient de plus en plus important pour faciliter le développement économique et social des États Membres, en particulier des pays en développement. Nous appelons la communauté internationale à prendre des mesures concrètes pour garantir l'application effective de la résolution.

Nous nous félicitons des engagements politiques et des mesures concrètes que les États Membres ont pris pour promouvoir la coopération internationale touchant les utilisations pacifiques, ainsi que des progrès accomplis dans le cadre des instances multilatérales et par les voies bilatérales, tout en notant la persistance de restrictions excessives limitant l'exportation vers les pays en développement de matières, équipements et technologies destinés à des fins pacifiques. Nous réaffirmons qu'il importe de promouvoir la coopération internationale à des fins pacifiques et de continuer de débattre de cette importante question dans le cadre de l'ONU, de manière ouverte et inclusive, et en recourant aux mécanismes et arrangements internationaux, régionaux et bilatéraux existants prévus à cet effet, conformément à la résolution. Nous demandons aux États Membres de poursuivre le dialogue sur la promotion des utilisations pacifiques et la coopération internationale en la matière, notamment en recensant les lacunes et les difficultés, mais aussi les idées et les possibilités, concernant le renforcement de la coopération et en explorant les pistes de progrès.

Nous présenterons un projet de résolution intitulé « Promotion de la coopération internationale touchant les utilisations pacifiques dans le contexte de la sécurité internationale » à l'Assemblée générale à sa soixante-dix-neuvième session, en 2024. Nous invitons tous les États à participer activement au processus de suivi.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Union européenne, en qualité d'observatrice.

M. Karczmarz (Union européenne) (*parle en anglais*) : J'ai l'honneur de prendre la parole au nom de l'Union européenne. La Macédoine du Nord, le Monténégro, la Serbie, l'Albanie, l'Ukraine, la République de Moldova et la Bosnie-Herzégovine, pays candidats, la Géorgie, candidat potentiel, l'Islande et la Norvège, pays de l'Association européenne de libre-échange et membres de l'Espace économique européen, ainsi que Monaco et Saint-Marin s'associent à cette déclaration.

Au cours de la dernière décennie, la communauté internationale a clairement établi que l'ordre international fondé sur des règles s'appliquait également au comportement des États dans le cyberespace. Tous les membres de l'Assemblée générale ont affirmé à plusieurs reprises leur soutien au cadre évolutif du comportement responsable des États dans le cyberespace, fondé sur la reconnaissance de l'applicabilité du droit international dans le cyberespace, l'adhésion à des normes volontaires et non contraignantes de comportement des États, le

renforcement des capacités et l'amélioration des mesures de confiance concrètes aux fins de la réduction du risque de conflit. Le large consensus international obtenu autour de ces quatre éléments est la principale réalisation de la cyberdiplomatie au cours de la dernière décennie.

La guerre d'agression illégale, injustifiée et non provoquée de la Russie a gravement remis en question l'ordre international fondé sur des règles, y compris dans le domaine cybernétique. Les cyberattaques destructrices lancées contre l'Ukraine, souvent associées à des attaques de missiles, sont sans précédent et ont des répercussions sur les pays de l'Union européenne. Au cours de l'année écoulée, l'Ukraine a non seulement été victime d'un plus grand nombre d'attaques de maliciels destructeurs de données que n'importe quel autre pays auparavant, mais elle a aussi réussi à en empêcher un grand nombre, grâce à sa cyberdéfense et sa résilience extraordinaires.

Le nouveau contexte de menace en Europe, induit par l'agression russe contre l'Ukraine, ainsi que d'autres menaces croissantes et évolutives émanant d'acteurs étatiques et non étatiques, influent sur la manière dont l'Union européenne aborde les cyberactivités malveillantes. Nous avons renforcé notre engagement à poursuivre la révision et l'amélioration constante de la cyberrésilience au sein de l'Union européenne et à élaborer de nouvelles stratégies sur la meilleure façon de faire face aux cybermenaces provenant de tous les acteurs malveillants.

Tout en reconnaissant que c'est aux États qu'il incombe au premier chef de garantir la paix et la sécurité internationales, d'autres parties prenantes ont un rôle essentiel à jouer à cet égard. Le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), créé en application de la résolution 75/240, est l'occasion pour la communauté internationale d'échanger de manière ouverte, inclusive et transparente sur l'utilisation responsable des technologies de l'information et de la communication par les États, dans le respect du droit international.

Nous nous félicitons du consensus obtenu en 2023 sur le rapport d'activité annuel du groupe de travail à composition non limitée (voir A/78/265), et soulignons que la communauté internationale doit poursuivre sur la voie du renforcement de la sécurité et de la stabilité du cyberespace. Le rapport d'activité annuel aurait pu aller plus loin, mais il présente toutefois plusieurs décisions et étapes à venir qui peuvent être considérées comme des moyens d'action concrets pour renforcer le cadre de comportement responsable des États dans le cyberespace et le droit international.

Beaucoup reste à faire, notamment pour soutenir la mise en œuvre pratique des résultats de ces discussions. L'Union européenne et ses États membres se réjouissent à l'idée de continuer à travailler avec les États et les autres parties prenantes pour faire avancer ces efforts, notamment au moyen d'un dialogue inclusif sur l'élaboration d'un programme d'action de l'ONU, en s'appuyant sur les résultats consensuels des groupes d'experts gouvernementaux et des groupes de travail à composition non limitée établis successivement au sein de l'Organisation, ainsi que sur les travaux du groupe de travail à composition non limitée actuellement en place et sur le rapport du Secrétaire général.

Le large soutien, apporté à la session de l'année dernière de la Première Commission, à la résolution 77/37, adoptée par 157 voix et coparrainée par un groupe interrégional de 74 pays, a réaffirmé la détermination des États à mettre en œuvre le cadre normatif convenu au moyen d'un mécanisme permanent, inclusif et orienté vers l'action. Il démontre clairement l'aspiration commune de la grande majorité des États à promouvoir la paix, la sécurité et la stabilité dans le cyberespace au moyen d'une instance permanente et coopérative qui favorise l'échange de connaissances et des meilleures pratiques, évite la duplication des efforts et contribue aux efforts de mise en œuvre nationaux et régionaux. Plus de 40 États, issus de tous les groupes régionaux, ont fait part de leurs observations écrites, et le Secrétaire général a publié un rapport (A/76/77) qui offre un contenu de fond et des recommandations de grande valeur pour la poursuite d'un dialogue inclusif sur le programme d'action.

Comme indiqué dans la résolution 77/37 adoptée l'année dernière, le programme proposé vise à offrir aux États une certaine souplesse pour traiter des questions pour lesquelles des discussions politiques, des échanges d'informations et une mise en œuvre pratique seraient utiles. Le programme sera dirigé par les États et cherchera également à favoriser la concertation multipartites ; il prévoit des consultations régulières avec les parties prenantes concernées, y compris le secteur privé, le monde universitaire et la société civile, afin qu'elles examinent ces questions et apportent leurs points de vue singuliers. De nombreuses parties prenantes non étatiques mènent déjà des initiatives propres à instaurer la confiance entre les États et les acteurs non étatiques, et leur participation permettra d'obtenir de meilleurs résultats et contribuera à la transparence, à la crédibilité et à la pérennité de la mise en œuvre du cadre.

Plus important encore, la mise en place d'une instance permanente permettrait à la communauté internationale d'axer ses discussions sur le fond et sur le

renforcement de la coopération et de la confiance entre les États plutôt que d'avoir des débats récurrents sur les processus à venir. Nous ne devons pas manquer cette occasion de faire avancer nos travaux dans un environnement stable, et l'Union européenne et ses États membres soutiennent pleinement la résolution correspondante présentée à l'Assemblée générale à cette fin. Pour maintenir en place un processus à voie unique à l'ONU, nous avons besoin d'un mécanisme permanent, qui devrait être établi après la fin du mandat de l'actuel groupe de travail à composition non limitée (2021-2025), et dont la portée, la structure et la teneur doivent être définies sur la base des discussions tenues au sein dudit groupe en 2024 et 2025.

Compte tenu de l'augmentation des cybermenaces internationales, il est plus important que jamais de renforcer notre cybercollaboration avec des partenaires internationaux, ainsi que de promouvoir une compréhension commune de la manière dont le droit international s'applique dans le cyberespace et de la façon de continuer d'appliquer le cadre de comportement responsable des États dans le cyberespace élaboré sous les auspices de l'ONU. C'est pourquoi l'Union européenne soutient le projet de résolution A/C.1/78/L.60, présenté par la France, qui vise à créer, sous l'égide de l'Organisation, un mécanisme au sein duquel les États Membres de l'Organisation pourront, avec souplesse, tenir des discussions pratiques sur la meilleure façon de sécuriser le cyberespace pour tous. Nous ne pourrons garantir effectivement un cyberespace ouvert, stable et sûr qu'à condition de collaborer, d'améliorer la coordination et la complémentarité, de briser les cloisonnements et de créer des méthodes nouvelles et innovantes pour lutter contre les comportements malveillants dans le cyberespace. Cette démarche est au cœur de l'ambition de l'Union européenne.

M. Lagardien (Afrique du Sud) (*parle en anglais*) : L'Afrique du Sud s'associe à la déclaration faite au nom du Mouvement des pays non alignés.

L'Afrique du Sud se félicite de l'adoption par consensus du deuxième rapport d'activité annuel (voir A/78/265) du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Ce processus a joué un rôle important dans l'instauration d'une confiance mutuelle et la promotion d'une coopération pacifique entre les États. En ce qui concerne les nouvelles menaces auxquelles sont confrontés les États, nous estimons que des mesures de coopération sont nécessaires pour faire face aux dangers qui pèsent sur les infrastructures numériques.

Nous avons participé de bonne foi au groupe de travail à composition non limitée afin de garantir que le dialogue entre les États se déroule sous les auspices de l'ONU, un cadre universel et multilatéral qui favorise le règlement pacifique des différends. L'Afrique du Sud estime que le maintien de la paix et de la sécurité internationales dans le cyberespace est une responsabilité collective. Nous sommes d'avis que les États devraient utiliser les 11 règles, normes et principes existants de comportement responsable des États dans le cyberespace dans leur forme actuelle pendant que nous étudions la possibilité d'un cadre de coopération plus large.

Le deuxième rapport d'activité annuel nous offre deux mesures primordiales de renforcement de la confiance : la poursuite des travaux visant à établir un dialogue institutionnel régulier et le répertoire d'interlocuteurs. Nous considérons également le groupe de travail à composition non limitée et ses résultats consensuels comme une mesure de confiance en soi, et nous félicitons le Président du groupe, l'Ambassadeur Burhan Gafoor, et son équipe des efforts qu'ils déploient pour garantir que nous obtenions des résultats tangibles et que le processus reste orienté vers l'action. Les discussions sur les différents formats d'échange de vues entre les États en ce qui concerne les menaces potentielles et émergentes nous ont montré que la communauté internationale peut continuer à dialoguer de manière constructive pendant les périodes politiques difficiles. Dans cette optique, l'Afrique du Sud soutient les propositions visant à créer un répertoire des menaces et un portail mondial de coopération en matière de cybersécurité. Nous espérons que les prochaines sessions du groupe de travail à composition non limitée permettront d'approfondir ces idées.

Nous sommes d'avis que des exposés présentés par les experts compétents des organisations régionales et sous-régionales, des entreprises, des organisations non gouvernementales et des milieux intellectuels, compte étant dûment tenu d'une représentation géographique équitable, seraient utiles au processus intergouvernemental, mais nous savons que le Président du groupe de travail a utilisé son pouvoir de mobilisation pour inviter différentes parties prenantes à exprimer leurs vues sur la façon de garantir la sécurité du numérique. Le groupe de travail à composition non limitée a donc été en mesure de prendre en considération le plus grand nombre possible de points de vue différents dans le cadre de ses travaux.

En tant que pays en développement, l'Afrique du Sud retire des avantages de l'échange de vues entre les États au sein du groupe de travail à composition non limitée ; nous soutenons dès lors le Président et le calendrier qu'il a proposé en vue de faciliter le processus de concertation sur l'avenir de nos discussions en tant que

communauté internationale. L'Afrique du Sud estime qu'il est vital pour la communauté internationale de préserver les processus existants, tels que ceux qui ont fait leurs preuves durant les périodes difficiles.

M. Alqaisi (Jordanie) (*parle en arabe*) : Tout d'abord, je voudrais, au nom du Groupe des États arabes, réaffirmer la nécessité de mettre un terme à la guerre et à l'agression brutale que mène Israël dans la bande de Gaza. Nous condamnons cette agression dans les termes les plus fermes. Un accès sûr et durable à l'aide humanitaire et médicale essentielle doit être garanti, de même que la fin des déplacements forcés de Palestiniens.

En ce qui concerne le débat thématique d'aujourd'hui, le Groupe des États arabes s'associe à la déclaration faite au nom du Mouvement des pays non alignés.

En ce qui concerne les autres mesures de désarmement, le Groupe des États arabes souligne que les solutions convenues dans le cadre multilatéral et conformément à la Charte des Nations Unies constituent le seul moyen durable d'aborder les questions de désarmement et de sécurité internationale. Le Groupe appelle tous les États Membres à réaffirmer et à mettre en œuvre les engagements individuels et collectifs qu'ils ont pris dans le cadre international multilatéral. Nous réaffirmons notre confiance dans le rôle central de l'ONU en matière de désarmement et de non-prolifération.

Le Groupe des États arabes exprime sa préoccupation face à l'augmentation, sur le plan mondial, des tensions et des dépenses militaires, alors qu'une grande partie de ces dernières pourrait être consacrée à la promotion du développement durable et à l'élimination de la pauvreté dans le monde, en particulier dans les pays en développement, y compris les pays arabes. Le Groupe réaffirme qu'il importe d'assurer le suivi du Programme d'action adopté en 1987 à la Conférence internationale sur la relation entre le désarmement et le développement, ainsi que des effets de la hausse des dépenses militaires sur la réalisation des objectifs de développement durable, conformément au Programme de développement durable à l'horizon 2030.

Le fait que des États continuent de détenir et de moderniser des arsenaux nucléaires constitue une menace grave pour la paix et la sécurité internationales et le développement durable. Le Groupe des États arabes souligne donc que les instances internationales de désarmement doivent prendre en compte les normes pertinentes lors de la négociation des traités et conventions sur le désarmement et la maîtrise des armements. Tous les États doivent contribuer à garantir le respect des normes environnementales dans l'application de ces traités et conventions.

En ce qui concerne la cybersécurité, le Groupe des États arabes se déclare préoccupé par l'utilisation accrue du numérique dans des activités destructrices qui portent atteinte à la paix et à la sécurité internationales, notamment les activités menées par des organisations terroristes et criminelles. Le Groupe souligne que l'ONU doit continuer à élaborer des règles contraignantes qui régissent le comportement responsable des États dans l'utilisation du numérique, à un rythme qui suive l'évolution rapide de ce domaine vital. Il est également nécessaire de poursuivre la coopération internationale et de préserver le rôle central de l'Organisation dans ces efforts.

Le Groupe des États arabes souligne qu'il importe de poursuivre la coopération internationale pour promouvoir la sécurité du numérique. Cela renforcerait les capacités des États de contrer d'éventuels actes de sabotage. De nombreux rapports publiés par divers groupes d'experts gouvernementaux et groupes de travail à composition non limitée ont mis l'accent sur ces attaques. Le Groupe tient à assurer le rôle central de l'Organisation des Nations Unies dans la promotion des normes internationales relatives à la sûreté et à la sécurité du numérique et à poursuivre la coopération avec l'Organisation sur cette question, qui affecte toutes les installations vitales de divers États, compte tenu de l'utilisation accrue du numérique dans des actes de sabotage qui menacent la sécurité internationale.

Pour conclure, le Groupe des États arabes souligne sa volonté de participer activement au groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), créé en application de la résolution 75/240. Le Groupe se félicite de l'adoption par consensus du deuxième rapport d'activité annuel du groupe de travail à composition non limitée (voir A/78/265) et attend avec intérêt de mener des débats ciblés sur les différentes propositions pertinentes visant à aider les pays en développement à faire face aux menaces croissantes liées à l'utilisation du numérique.

M. Sirie (Indonésie) (*parle en anglais*) : L'Indonésie 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. À cet égard, je voudrais ajouter quelques observations à titre national.

Ma première remarque concerne l'importance de renforcer les mesures de coopération dans le domaine de la sécurité du numérique. La technologie est souvent décrite comme une arme à double tranchant, un outil précieux qui s'accompagne de risques importants. Or, à mesure que nous devenons plus interconnectés,

les cyberattaques apparaissent comme une menace majeure pour l'infrastructure numérique, provoquant des interruptions de service, des vols de données et des fraudes. À cet égard, l'Indonésie souligne la nécessité de mesures de coopération entre tous les États Membres pour garantir un cyberespace sûr, sécurisé et stable.

L'Indonésie réaffirme son soutien aux travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), notamment à la priorité qu'il accorde au renforcement des capacités et de la confiance. Cela aidera les pays à renforcer leurs capacités en matière de cybersécurité. Pour sa part, l'Indonésie a lancé, en juillet, sa stratégie nationale de cybersécurité, qui donne davantage de moyens à l'organisme national de cybersécurité nouvellement créé et complète le cadre juridique visant à protéger les utilisateurs d'ordinateurs, les infrastructures nationales critiques et le cyberespace au moyen de lois, telle que la loi sur la confidentialité des données de 2022 et la loi sur l'information et les transactions électroniques de 2008. L'Indonésie attend avec intérêt la poursuite du débat sur le renforcement des capacités en matière de cybersécurité au sein du groupe de travail à composition non limitée.

Ma deuxième remarque concerne le renforcement des cadres et normes multilatéraux sur l'utilisation du numérique. Dans l'environnement actuel de la sécurité internationale, la coopération fondée sur le consensus semble s'amoindrir. Nous ne devons pas laisser cela se produire dans le domaine de la sécurité du numérique. Une telle tendance permettrait aux acteurs malveillants de perturber la sécurité du cyberespace, menaçant ainsi la paix et la stabilité internationales. Dès lors, compte tenu de la situation précaire de notre environnement international, l'Indonésie salue l'effort consenti par les États Membres pour adopter par consensus le deuxième rapport d'activité annuel du groupe de travail à composition non limitée (voir A/78/265). Grâce à son approche inclusive et progressive, le groupe de travail a su s'imposer comme une instance qui facilite la coopération, la transparence et les mesures de confiance sur la question de la sécurité du numérique. L'Indonésie se félicite également de la création du répertoire d'interlocuteurs, un résultat concret et tangible du groupe de travail, et attend avec intérêt sa mise en service. Il est donc impératif de préserver l'intangibilité du groupe de travail en tant que cadre inclusif pour la gestion des cyberrisques et la promotion de la bonne gouvernance et des bonnes pratiques dans le cyberespace.

Alors que nous sommes à mi-parcours du mandat du groupe de travail à composition non limitée, je souhaite m'associer aux délégations qui ont suggéré que soit rédigé un projet de résolution concernant le futur mécanisme de délibération sur la sécurité du numérique. Il importe que nous restions fidèles aux éléments communs du futur mécanisme convenus par consensus dans le deuxième rapport d'activité annuel. Nous devons éviter la présentation de projets de résolution concurrents sur le même sujet, qui entraîneraient une fragmentation des travaux de la Première Commission, car cela donnerait lieu à des processus parallèles qui nuiraient aux travaux du groupe de travail. Au contraire, nous devons continuer de recourir au groupe de travail pour examiner les questions de la coopération soutenue entre les pays et de la mise en commun des meilleures pratiques et des capacités afin de relever efficacement les défis de la cybersécurité, de réduire la fracture numérique et de permettre un progrès socioéconomique sans entrave.

M. Hegazy (Égypte) (*parle en anglais*) : Je tiens tout d'abord à dire que nous condamnons fermement le fait que les Palestiniens de Gaza continuent d'être pris pour cible. Nous réitérons nos appels à un cessez-le-feu urgent et inconditionnel, et demandons à Israël de mettre immédiatement fin à ses tentatives de déplacer de force plus d'un million de civils dans le sud de la bande de Gaza. Israël doit également permettre l'accès sans entrave de l'aide humanitaire afin d'alléger les souffrances humaines du peuple palestinien.

L'Égypte s'associe aux déclarations prononcées au nom du Mouvement des pays non alignés et du Groupe des États arabes, et souhaite formuler les observations suivantes.

L'Égypte réaffirme que les instruments non discriminatoires, multilatéraux et juridiquement contraignants sont les mesures les plus efficaces pour réaliser des progrès durables dans le domaine du désarmement et de la sécurité internationale. Pour maintenir la paix et la sécurité internationales, éviter le chaos et garantir l'évolution fiable des technologies concernées et leur contribution au développement et au bien-être, il est indispensable que tous les États continuent de respecter les engagements pris antérieurement, ainsi que le droit international, a fortiori au vu de la rapidité des innovations scientifiques et technologiques dans plusieurs domaines stratégiques ayant une incidence directe sur la sécurité internationale, pour lesquels des règles claires qui éviteraient qu'ils ne deviennent le théâtre d'une course aux armements et de conflits armés n'ont pas été convenues au niveau international.

Le cyberespace, l'espace extra-atmosphérique et les applications de l'intelligence artificielle, notamment dans le domaine des armes létales autonomes, en sont

des exemples marquants. L'absence de progrès dans la lutte contre les graves menaces qui pèsent sur la sécurité dans ces domaines est clairement due non pas à un manque de compétences techniques de la communauté internationale, mais plutôt à la conviction, malavisée et persistante, de certains États qu'une domination absolue dans ces domaines peut être maintenue. Ces États opposent ainsi une résistance à tout effort pour élaborer des régimes internationaux équitables qui interdisent l'utilisation malveillante et la militarisation de ces technologies, lesquelles conduiraient à une course aux armements que personne ne pourrait gagner.

Nous nous félicitons que le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), créé en application de la résolution 75/240, ait mené à bien sa deuxième session annuelle et adopté son deuxième rapport d'activité annuel (voir A/78/265), ainsi que le document intitulé « Éléments concernant l'élaboration et la mise en service d'un répertoire mondial et intergouvernemental d'interlocuteurs », et d'autres recommandations tournées vers l'avenir qui pourraient ouvrir la voie à des discussions ciblées sur les questions et propositions en suspens relevant de la compétence du groupe du travail.

De nombreuses idées créatives et propositions constructives ont été présentées au groupe de travail à composition non limitée, y compris la tenue d'un dialogue institutionnel régulier sous les auspices de l'ONU, par exemple sur la possible mise en place d'un programme d'action de l'Organisation sur l'utilisation du numérique dans le contexte de la sécurité internationale, une proposition que l'Égypte présente avec la France depuis 2020 et qui a été élaborée avec le soutien d'un groupe interrégional d'États dans le but de compléter les travaux du groupe de travail après la conclusion de son mandat, fin 2025.

Dans ce contexte, l'Égypte a présenté sa position nationale sur le futur mécanisme de dialogue institutionnel régulier sur le site Web du groupe de travail. Nous partageons le point de vue selon lequel tout processus futur à ce sujet doit contenir un pilier distinct sur la mise en œuvre du cadre convenu et prévoir le renforcement des capacités des pays en développement à cet égard. Ce mécanisme, placé sous l'égide de l'Organisation, doit être flexible, orienté vers l'action, à voie unique, permanent et fondé sur le consensus, comme l'indique le paragraphe 55 du deuxième rapport d'activité annuel du groupe de travail à composition non limitée, adopté par consensus. Il doit permettre de recenser les éventuelles lacunes du cadre existant et de les combler par la mise en œuvre de décisions consensuelles, de renforcer la coopération et l'assistance internationales et de développer davantage le cadre existant de normes, règles et principes, en plus des obligations contraignantes.

Dans ce contexte, nous saluons le soutien croissant à l'idée de s'attacher à mettre en œuvre le cadre convenu et à le développer davantage. En outre, nous estimons qu'il nous faut continuer de soutenir l'actuel groupe de travail pour qu'il puisse mener à bien ses travaux, et consacrer nos efforts à la recherche d'un terrain d'entente pour la mise en place du futur mécanisme, en mettant à profit les travaux du groupe de travail. Dans cette optique, nous encourageons toutes les délégations à éviter de préjuger de l'issue des négociations en cours ou d'imposer prématurément la mise en place de voies parallèles, non seulement dans le cadre du groupe de questions 5, mais aussi dans l'ensemble des questions traitées. Une telle démarche ne ferait qu'accentuer les divisions et les impasses.

M^me^ Gomez Sardinas (Cuba) (*parle en espagnol*) : Nous souscrivons à la déclaration faite par le représentant de l'Indonésie au nom du Mouvement des pays non alignés. Nous nous associons également à la déclaration faite par le représentant de la Chine sur la coopération internationale touchant les utilisations pacifiques dans le contexte de la sécurité internationale.

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, dans l'intérêt des générations présentes et futures. Nous appelons à l'adoption de nouvelles mesures en faveur du désarmement et de la sécurité internationale qui nous aident à construire un monde de paix le plus rapidement possible. Nous devons réduire les ressources considérables consacrées à la militarisation. Les fonds et les progrès scientifiques et technologiques qui servent actuellement à développer le complexe militaro-industriel, ainsi qu'à mettre au point, produire et perfectionner des armes de plus en plus sophistiquées, apporteraient d'innombrables avantages à l'humanité s'ils étaient utilisés pour la réalisation du Programme de développement durable à l'horizon 2030 et de ses objectifs.

Nous, États Membres, devons continuer d'œuvrer à préserver le multilatéralisme, principe de base des négociations sur le désarmement et la maîtrise des armements. Nous rappelons que ces négociations doivent respecter les normes internationales contraignantes relatives à l'environnement. Nous appuyons la négociation d'initiatives juridiquement contraignantes visant à empêcher la militarisation de l'espace et du cyberespace et à interdire l'emploi de systèmes d'armes létaux autonomes.

M. Lagardien (Afrique du Sud), Vice-Président, assume la présidence.

Nous soutenons les travaux en cours du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), qui permet aux États Membres d'examiner les questions de manière transparente, inclusive et dans des conditions d'égalité. Comme preuve de notre attachement à cette instance, nous approuvons l'adoption par consensus de son deuxième rapport d'activité annuel (voir A/78/265), même si nous avions de plus grands espoirs, en particulier s'agissant d'avancer dans l'élaboration de normes supplémentaires de comportement responsable des États dans le domaine de la sécurité du numérique. Nous ne devons pas préjuger des résultats des discussions sur le futur mécanisme de dialogue institutionnel régulier, ni promouvoir le programme d'action proposé au détriment d'autres initiatives nationales.

Les technologies de l'information et des communications (TIC) ne doivent pas être utilisées comme moyen de guerre, mais à des fins exclusivement pacifiques. Nous nous opposons à l'utilisation hostile des TIC dans l'objectif, déclaré ou non, de renverser l'ordre juridique et politique d'autres États ou de commettre ou inciter à commettre des actes de terrorisme. Nous rejetons l'emploi de la force comme réponse légitime à une cyberattaque.

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 que ce pays consacre à cet objectif. Nous condamnons l'utilisation des nouvelles technologies numériques et d'autres plateformes connexes pour déstabiliser notre pays, répandre de fausses informations sur la réalité cubaine et encourager un changement de régime à Cuba. Nous nous opposons à la manipulation du réseau Internet cubain, en violation des normes internationales en la matière. Nous demandons aux États-Unis de mettre immédiatement fin au blocus financier et commercial imposé à Cuba, qui limite considérablement l'accès aux TIC et leur utilisation au profit du peuple cubain.

Nous sommes convaincus qu'un désarmement général et complet, en particulier un désarmement nucléaire, est nécessaire et possible. Cuba continuera de promouvoir l'adoption de mesures efficaces qui nous permettent d'atteindre ce noble objectif.

M. Pieris (Sri Lanka) (*parle en anglais*) : Sri Lanka s'associe à la déclaration faite par le représentant de l'Indonésie au nom du Mouvement des pays non alignés. Je prononce la présente déclaration à titre national.

La troisième décennie du XXIe siècle se caractérise essentiellement par des progrès rapides et des révolutions dans le domaine du numérique. Nous nous trouvons en effet à un moment crucial de l'ère numérique, et dans un monde qui tire parti des avantages offerts par ces technologies. Aujourd'hui, le numérique est plus que jamais intrinsèquement lié à notre vie quotidienne. L'espace virtuel dans lequel nous évoluons au quotidien, des États jusqu'aux individus, témoigne du rôle vital que jouent désormais ces technologies. S'étant répandu dans toutes les sphères de l'activité humaine, le numérique est désormais un outil pour tous les domaines de cette activité.

Dans mon pays, un programme intitulé « DIGIECON Sri Lanka 2023-2030 » a été lancé en mai avec la ferme résolution de transformer le pays en un pays numériquement inclusif, ce qui met en lumière la très forte synergie entre le numérique et le progrès économique à Sri Lanka. Ce programme, qui comprend un plan directeur et un cadre réglementaire en matière numérique, ainsi qu'une série d'événements annuels, vise à accélérer la transition de l'économie sri-lankaise vers une économie numérique inclusive en tirant parti de solutions basées sur des technologies avancées.

Tout en préfigurant ces limites et malgré tous les aspects positifs du cyberespace, celui-ci est également devenu, comme d'autres formes de technologies porteuses de transformation, un refuge pour divers acteurs qui se livrent à des activités criminelles et terroristes, ainsi que pour ceux qui ont des intérêts particuliers à propager la haine, l'intolérance et l'incitation à la violence, en particulier sur les médias sociaux. Ces derniers temps, des niveaux de vulnérabilité sans précédent ont été observés face aux cyberattaques et à d'autres activités malveillantes ciblant les services numériques, qui permettent de perturber des millions de vies en appuyant sur quelques boutons.

Sri Lanka appuie à ce titre la tenue de délibérations multilatérales au sein du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), créé en application de la résolution 75/240. Il s'agit du seul mécanisme inclusif, élaboré sous les auspices de l'ONU, prévoyant une participation active et égale de tous les États. Nous nous félicitons de l'adoption par le groupe de travail de son deuxième rapport d'activité annuel (voir A/78/265) et de la mise en place du répertoire mondial et intergouvernemental d'interlocuteurs, et nous attendons avec intérêt les futures délibérations du groupe de travail. Nous suivons également avec attention les débats en cours au

sein du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

Nous soulignons que l'utilisation du numérique doit pleinement respecter 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, de respect des droits humains et d'adhésion au principe bien établi de la coexistence pacifique entre les États. C'est donc aux États concernés qu'il incombe au premier chef d'adopter des lois et de prendre des mesures pour prévenir les activités illicites et criminelles visant des particuliers, des entreprises ou des organismes publics, mais de nombreux pays en développement, dont le mien, sont confrontés à cet égard à des contraintes de capacité.

La créativité humaine est bien connue. La capacité des humains à s'autodétruire par leur propre créativité et la poursuite d'intérêts personnels à court terme est également bien connue, que ce soit par l'utilisation malveillante de technologies existantes ou par l'invention de nouvelles technologies, telles que l'intelligence artificielle ou les systèmes d'armes létaux autonomes. Nous ne pouvons pas nous permettre de mésaventures qui mettent en péril notre existence même.

M^me^ Lipana (Philippines) (*parle en anglais*) : Les Philippines s'associent aux déclarations faites par le représentant de la Thaïlande, au nom de l'Association des nations de l'Asie du Sud-Est, et par le représentant de l'Indonésie, au nom du Mouvement des pays non alignés. J'aimerais faire les observations suivantes à titre national.

Nous soutenons fermement le projet de résolution A/C.1/78/L.4 sur la relation entre le désarmement et le développement, présenté au nom du Mouvement des pays non alignés, qui souligne l'importance d'aligner le désarmement sur les objectifs de développement mondiaux. Le projet de résolution appelle à la réduction des dépenses militaires et à la réorientation des ressources vers le développement économique et social, afin de réduire l'écart entre les pays développés et les pays en développement. Il souligne la symbiose entre le désarmement et le développement et le rôle de la sécurité dans l'instauration de la paix et de la prospérité.

Les Philippines soutiennent pleinement le projet de résolution A/C.1/78/L.6 sur les normes environnementales et le désarmement, présenté au nom du Mouvement des pays non alignés, qui souligne le lien crucial entre la protection de l'environnement et la sécurité mondiale et encourage un désarmement responsable en mettant l'accent sur la préservation de l'environnement. Les Philippines s'associent au Mouvement des pays non alignés pour souligner l'importance du multilatéralisme dans les efforts de désarmement et de non-prolifération, et insistent sur le pouvoir de négociations transparentes et de la coopération entre les États pour préserver la paix et la sécurité mondiales.

En ce qui concerne la sécurité et l'utilisation du numérique, les Philippines soutiennent pleinement le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Nous soulignons les effets positifs du numérique sur le développement et la nécessité d'un comportement responsable des États pour garantir la stabilité et la sécurité du cyberespace. Les Philippines déplorent l'utilisation malveillante du numérique, en violation du droit international, et appellent à des efforts collectifs pour sauvegarder le cyberespace et promouvoir son utilisation pacifique.

Nous approuvons le deuxième rapport d'activité annuel du groupe de travail à composition non limitée (voir A/78/265). Le groupe de travail, qui fonctionne sur la base du consensus et associe tous les États Membres, a réussi à produire des résultats orientés vers l'action afin de renforcer la confiance entre les nations sur les questions de cybersécurité. Les Philippines soutiennent pleinement la poursuite fructueuse des activités de ce mécanisme qui, sous sa forme actuelle, répond aux préoccupations et aux intérêts de tous les États Membres de l'ONU en matière de cybersécurité. Nous sommes favorables à un mécanisme permanent à voie unique, dirigé par les États et placé sous l'égide de l'Organisation, qui ferait rapport à la Première Commission. Ce mécanisme doit être ouvert, inclusif, transparent, durable et flexible pour s'adapter à l'évolution des besoins des pays en développement dans l'environnement numérique dynamique. Nous espérons que nous pourrons tous harmoniser nos efforts à cette fin dans le cadre de nos délibérations actuelles et futures sur les questions de cybersécurité.

Comme nous l'avons entendu tout au long des consultations informelles, des projets de résolution concurrents ne sont pas utiles. Ils sèment la discorde. À cet égard, dans un esprit de rapprochement, nous avons été et restons déterminés à aider à trouver un terrain d'entente, et les Philippines continueront à dialoguer avec les partisans d'un futur mécanisme qui pourrait bénéficier du soutien le plus large possible et avec les délégations intéressées à travailler à cette fin.

En ce qui concerne les systèmes d'armes létaux autonomes, les Philippines soutiennent pleinement le projet de résolution A/C.1/78/L.56. Nous félicitons la communauté internationale d'avoir reconnu la nécessité urgente de résoudre les problèmes posés par les systèmes d'armes autonomes, qui soulèvent des questions humanitaires, juridiques, sécuritaires, technologiques et éthiques. Face au développement rapide de ces technologies, il est essentiel de faire respecter le droit international et de maintenir les normes d'humanité les plus élevées. Le caractère inclusif du projet de résolution, lequel prend en compte diverses perspectives, garantit une approche globale pour traiter cette question essentielle. Le fait de charger le Secrétariat de préparer sur le sujet un rapport complet qui tienne compte des avancées technologiques et associe diverses parties prenantes démontre l'engagement de la communauté internationale à faire respecter le droit international et à sauvegarder la paix et la sécurité. Les Philippines estiment que le projet de résolution catalysera les efforts multilatéraux collectifs visant à relever les défis posés par les systèmes d'armes létaux autonomes. Nous attendons avec intérêt la poursuite des discussions et des progrès sur cette question dans le cadre de la Convention sur certaines armes classiques.

En conclusion, les Philippines sont fermement attachées à forger un avenir de sécurité, de développement et d'utilisation responsable des technologies. Nous nous engageons à apporter un soutien indéfectible aux principes du désarmement et du développement durable, en tirant parti de la force du multilatéralisme. En outre, nous insistons sur la nécessité de préserver le domaine numérique, en garantissant l'utilisation pacifique des technologies connexes et en maintenant la sécurité du cyberespace.

Enfin, nous soutenons les efforts de la communauté internationale visant à relever les défis éthiques et sécuritaires posés par les armes létales autonomes. Ensemble, nous pouvons résoudre ces problèmes complexes, en faisant respecter le droit international et les normes d'humanité les plus élevées.

M. Sivamohan (Malaisie) (*parle en anglais*) : La Malaisie s'associe aux déclarations faites par le représentant de l'Indonésie, au nom du Mouvement des pays non alignés, et par le représentant de la Thaïlande, au nom de l'Association des nations de l'Asie du Sud-Est.

La dépendance sans précédent de la société mondiale à l'égard des technologies de l'information et des communications (TIC) nécessite que l'on porte une attention soutenue aux questions de sécurité, qui dépassent les frontières nationales, tandis que l'utilisation accrue des TIC offre de nouvelles possibilités de promouvoir des objectifs communs. Les risques et les problèmes posés par l'utilisation malveillante des TIC doivent être traités efficacement. À cet égard, la Malaisie salue les efforts constants déployés par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Nous nous félicitons de l'adoption, en juillet, du deuxième rapport d'activité annuel du groupe de travail (voir A/78/265), qui constitue une base solide pour les travaux du groupe au cours de l'année à venir.

Nous constatons avec satisfaction que les États Membres sont convenus des éléments relatifs à l'élaboration et à la mise en service d'un répertoire mondial et intergouvernemental d'interlocuteurs. La Malaisie attend également avec intérêt la tenue de nouvelles discussions ciblées au sein du groupe de travail sur, entre autres, les menaces que les TIC font peser sur les infrastructures critiques et les infrastructures informatiques critiques, l'intégration des principes convenus de renforcement des capacités numériques et l'application du droit international dans l'utilisation des TIC.

La Malaisie reste déterminée à participer activement aux travaux du groupe de travail, qui s'est avéré être une instance très utile pour débattre des questions relatives à la sécurité du numérique entre tous les États Membres, avec les contributions des parties prenantes concernées. Il convient de préserver l'intégrité, l'efficacité et la crédibilité du groupe de travail à composition non limitée tandis que nous étudions des formats possibles de dialogue institutionnel régulier pour la période postérieure à 2025.

Il est rassurant de constater, comme l'indique le deuxième rapport d'activité annuel du groupe de travail, que les États Membres sont convenus, en principe, d'éléments communs sur lesquels serait fondé un futur mécanisme de dialogue institutionnel régulier. Parmi ces éléments figure notamment :

> « un mécanisme permanent à voie unique, dirigé par les États et placé sous l'égide de l'Organisation des Nations Unies, qui ferait rapport à la Première Commission » (*A/78/265, annexe, para. 55 a)*).

Les États Membres ont également :

> « reconnu l'importance du principe du consensus, tant pour la mise en place du futur mécanisme que pour ses processus décisionnels » (*ibid., para. 56*).

À cet égard, la Malaisie réaffirme qu'il convient d'éviter les processus parallèles au niveau multilatéral dans les domaines clefs du désarmement et de la sécurité internationale. C'est une question qui préoccupe particulièrement les petites délégations des pays en développement, compte tenu des contraintes de ressources financières et humaines.

Dans un contexte de nouvelles tensions entre grandes puissances et de déficit de confiance, le groupe de travail à composition non limitée a obtenu des résultats tangibles de manière progressive et par consensus. Cela témoigne de la bonne foi avec laquelle toutes les délégations ont participé au processus. Malgré les divergences de vues sur des questions particulières relevant de sa compétence, il est clair que le groupe de travail constitue en soi une mesure de confiance essentielle. Alors que nous examinons diverses propositions sur la voie à suivre, nous devons continuer à travailler de manière constructive pour garantir que le groupe de travail réalise son plein potentiel conformément à son mandat. Ma délégation espère vivement que le groupe de travail à composition non limitée restera, jusqu'à la fin de son mandat, une instance à voie unique, ouverte et inclusive, capable de répondre avec souplesse aux besoins des États Membres dans le domaine en rapide évolution de la sécurité du numérique.

M. in den Bosch (Royaume des Pays-Bas) (*parle en anglais*) : Outre la déclaration faite au nom de l'Union européenne, je voudrais faire les remarques suivantes à titre national.

Les technologies de l'information et des communications (TIC) sont des facteurs de développement durable importants et peuvent avoir des effets positifs sur la vie humaine. Mais le risque que ces technologies soient utilisées à mauvais escient par des acteurs étatiques et non étatiques augmente en même temps que notre dépendance à leur égard. C'est pourquoi il est essentiel non seulement que nous défendions les règles et les normes qui régissent l'utilisation des TIC par les États, mais aussi que nous les renforcions. Nous devons exploiter le potentiel des technologies numériques pour favoriser le développement économique et social tout en garantissant la sécurité et le bien-être des sociétés et des individus.

Face à ces difficultés, les États ont élaboré un cadre cumulatif et évolutif aux fins du comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. Ce n'est pas un mince exploit. Ce cadre est le fruit de négociations approfondies et d'efforts visant à instaurer la confiance entre les États ; il bénéficie donc de l'approbation de tous les États Membres de l'ONU. Le rapport d'activité annuel de 2023 (voir A/78/265) du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) constitue une nouvelle contribution importante à ce cadre en ce qu'il réaffirme l'applicabilité du droit international au cyberespace et réalise des progrès concrets sur la voie de la mise en place d'un répertoire d'interlocuteurs. Le rapport fournit des recommandations concrètes sur la mise en œuvre des normes de comportement responsable des États, renforce la nécessité de prendre en compte les questions de genre dans la lutte contre les menaces liées aux TIC et encourage un renforcement des capacités tenant compte des questions de genre. Dans cette optique, les Pays-Bas continueront à soutenir la participation des femmes au groupe de travail à composition non limitée, par le truchement du programme de bourses « Femmes dans le domaine de la cybersécurité ».

Nous saluons les travaux présentés dans le rapport, notamment l'approfondissement de la compréhension commune de la manière dont le droit international s'applique dans le cyberespace. Nous continuons également d'appuyer les travaux du groupe de travail à composition non limitée sur le renforcement des capacités pour faire progresser la mise en œuvre du cadre consensuel. Afin de consolider les mesures envisagées dans le rapport d'activité annuel du groupe de travail, les Pays-Bas espèrent que le projet de document de position de Singapour visant à approuver le rapport sera adopté sans vote.

Les Pays-Bas soutiennent l'initiative, prise dans le cadre du programme d'action, d'établir un mécanisme permanent, inclusif et orienté vers l'action après l'expiration, en 2025, du mandat de l'actuel groupe de travail à composition non limitée. Le programme d'action devra faire avancer les travaux vers deux objectifs : premièrement, continuer à élaborer at à parfaire le cadre normatif de comportement responsable des États sur la base du consensus, et, deuxièmement, favoriser la coopération internationale pour faire progresser la mise en œuvre de ce cadre évolutif. Ces deux objectifs ont également été mentionnés dans les conclusions du rapport du Secrétaire général sur le programme d'action (A/78/76), dans lequel ce dernier salue les projets de mécanisme orienté vers l'action qui font progresser la mise en œuvre du cadre normatif et qui soutiennent les capacités des États à le mettre en œuvre.

Dans leur contribution au rapport du Secrétaire général sur le programme d'action, les Pays-Bas ont proposé un mécanisme axé sur les besoins visant à faciliter le renforcement des capacités dans le cadre du programme d'action, qui mettrait à profit les initiatives existantes à l'intérieur et à l'extérieur du système des Nations Unies. Le projet est en cours d'élaboration et nous continuerons à en discuter avec les autres États Membres.

En ce qui concerne l'avancement de l'initiative relative au programme d'action, les Pays-Bas soutiennent fermement le projet de résolution A/C.1/78/L.60, déposé par la France. Le projet de résolution fixe un calendrier

et des objectifs clairs pour la mise en place d'un futur mécanisme de dialogue institutionnel régulier en 2026. Il encourage à parfaire l'élaboration du mécanisme au sein de l'actuel groupe de travail à composition non limitée et adopte une approche équilibrée quant à l'éventuelle future nécessité de disposer d'obligations juridiquement contraignantes supplémentaires.

Pour terminer, les Pays-Bas se réjouissent à l'idée de poursuivre les travaux au sein du groupe de travail à composition non limitée et de réaliser des progrès tangibles vers un cyberespace plus ouvert, plus libre, plus sûr, plus interopérable et plus pacifique.

M. Fausto Gonzalez (Mexique) (*parle en espagnol*) : Le Mexique attache une importance particulière à l'approche de l'utilisation responsable et pacifique de l'espace extra-atmosphérique. À l'ère numérique, où la majorité des activités humaines sont interconnectées dans le cyberespace, nous devons reconnaître qu'un comportement irresponsable dans cette sphère peut entraîner des cyberattaques, des tensions géopolitiques, voire des conflits.

C'est pourquoi le Mexique réaffirme qu'il est urgent de s'assurer que le cyberespace reste ouvert, libre, stable, sûr, accessible et résilient pour tous. Comme nous pouvons le voir, la nécessité de faire respecter le droit international, y compris le droit international humanitaire, dans le cyberespace est indéniable. Nous sommes fermement attachés à la mise en œuvre rigoureuse de normes et de principes de comportement responsable des États dans ce domaine. Nous constatons à cet égard qu'il est nécessaire d'équilibrer les préoccupations en matière de cybersécurité avec la protection des droits de l'homme et la promotion du développement par l'utilisation du numérique.

Pour les pays en développement, la réglementation du cyberespace n'est pas seulement une question de sécurité, mais plutôt une condition préalable à l'utilisation durable du cyberespace au sens large. Le cyberespace est un outil qui, s'il est correctement utilisé et réglementé, a le pouvoir de promouvoir l'innovation, de garantir un accès équitable à l'information, de renforcer notre économie numérique et de combler les inégalités en place dans notre monde.

La possibilité d'une course aux capacités offensives dans le cyberespace est une préoccupation de longue date que nous partageons avec de nombreux autres États. Il est alarmant de penser que des nations ou même des entités privées peuvent développer des capacités offensives avancées qui pourraient conduire à des actes de déstabilisation. À cet égard, le Mexique appelle à un engagement collectif pour éviter que le cyberespace ne devienne un terrain de plus où les rivalités s'expriment.

Le Président assume de nouveau la présidence.

Dans cet esprit, nous redisons notre confiance dans le multilatéralisme. Nous sommes convaincus que l'ONU, en particulier le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), est le format idéal pour continuer de relever ensemble les défis que posent le cyberespace et le numérique dans le contexte de la sécurité internationale. Nous soulignons les progrès significatifs réalisés au cours des discussions tenues au sein du groupe, en particulier l'adoption des deux rapports d'activité annuels et l'établissement et la mise en service du répertoire mondial d'interlocuteurs, ainsi que la formulation d'autres mesures visant à promouvoir la coopération et la confiance dans le cyberespace. Il est particulièrement important que le groupe de travail continue à favoriser la compréhension et le dialogue et à éviter la duplication des efforts au détriment de tous les pays.

Pour conclure, je lance un appel pour que nous continuions à mener des discussions productives et constructives qui débouchent sur un mécanisme de dialogue permanent sur le cyberespace. Le mécanisme doit être inclusif et permettre la participation de tous les acteurs concernés, ainsi que la coopération internationale, et il doit garantir le renforcement des capacités en fonction des différents besoins régionaux et sous-régionaux. Les discussions sur l'élaboration d'un mécanisme institutionnel permanent sur le cyberespace, qui envisagerait le renforcement des capacités et inclurait des normes de droit international, des règles et principes de comportement responsable des États, ainsi que des mesures de confiance, doivent continuer à figurer parmi les priorités du groupe de travail. Le Mexique espère que lors des prochaines sessions de fond du groupe de travail à composition non limitée, nous pourrons dégager encore plus de recommandations visant à garantir un cyberespace pacifique et équitable pour tous.

M^me^ Lukabyo (Australie) (*parle en anglais*) : Un cyberespace ouvert, sûr, stable, accessible et pacifique profite à tous. L'intérêt d'un cyberespace fondé sur des règles n'a jamais été aussi évident. Seul un cyberespace fondé sur des règles peut apporter la stabilité et l'indépendance nécessaires pour que tous les pays puissent déterminer leur propre avenir numérique et leur développement économique.

Cependant, jamais le cyberespace n'a été aussi contesté. Cette année encore, nous avons été témoins de cas inacceptables de cyberactivité malveillante, dans notre propre région Indopacifique et ailleurs, comme lorsque

la Russie prend l'infrastructure énergétique ukrainienne pour cible. Les questions cybernétiques sont devenues des questions stratégiques de politique étrangère qui sont une source de grande préoccupation pour tous les pays. Nous avons tous la responsabilité de travailler, ensemble et avec l'industrie, la société civile et la communauté technique, pour gérer les problèmes complexes liés à la sécurité internationale dans le cyberespace et de concentrer nos efforts sur la promotion de la paix et la prévention des conflits.

L'Australie reste fermement déterminée à œuvrer de manière collective pour faire face à ces difficultés, notamment dans le cadre de l'ONU. L'Organisation a toujours encouragé la coopération internationale pour comprendre les nouvelles menaces et réduire les menaces sur la paix et la sécurité internationales.

Nous réaffirmons une fois de plus notre engagement à agir conformément au cadre de comportement responsable des États dans le cyberespace, élaboré et approuvé grâce aux rapports de consensus adoptés par les groupes d'experts gouvernementaux et les groupes de travail à composition non limitée établis sous l'égide de l'ONU. L'Australie continuera à communiquer publiquement sur la façon dont elle met en œuvre, interprète et respecte ce cadre. La transparence favorise la responsabilité, la prévisibilité et la stabilité, et nous encourageons par conséquent tous les États à s'acquitter pleinement des engagements qu'ils ont pris au titre du cadre et à les respecter fidèlement.

L'Australie se réjouit que, à la cinquième session du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), les femmes aient été très représentées et que les parties prenantes aient montré une forte mobilisation. L'Australie se félicite du rapport d'activité annuel du groupe de travail (voir A/78/265) et de sa réaffirmation sans équivoque du cadre. Nous encourageons tous les États à s'impliquer véritablement dans les prochaines étapes recommandées dans le rapport, en particulier les recommandations visant à ce que les États continuent de mener des discussions ciblées sur la manière dont le droit international s'applique dans le cyberespace.

L'Australie accorde une grande importance aux résultats consensuels obtenus à l'ONU sur les questions cybernétiques, car ces questions sont tout simplement trop importantes pour être réparties sur plusieurs fronts. L'Australie plaide depuis longtemps en faveur de la mise en place d'un mécanisme permanent de l'Organisation pour avancer sur la question du comportement responsable des États dans le cyberespace, un mécanisme qui soit inclusif, transparent, démocratique et fondé sur le consensus.

Nous saluons l'initiative de la France, qui a déposé le projet de résolution A/C.1/78/L.60 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, programme qui nous permettrait de faire face de manière efficace aux nouvelles menaces qui pèsent sur la sécurité internationale. L'Australie souligne qu'un nouveau mécanisme permanent ne ferait pas concurrence à ceux qui l'ont précédé. Le mode et la structure des discussions tenues à l'ONU sur les questions cybernétiques ont considérablement évolué depuis la création du premier groupe d'experts gouvernementaux en 2004, qui se composait de 15 experts étatiques débattant à huis clos, jusqu'à la création ad hoc, en 2018, des groupes de travail à composition non limitée, qui sont ouverts à l'ensemble des 193 États Membres de l'Organisation. Le programme d'action représente la prochaine évolution des débats des Nations Unies sur le cyberespace ; il s'appuie sur ce qui a été fait auparavant et garantit que ces questions se verront accorder l'attention et l'importance qu'elles méritent à l'avenir.

Nous devons aussi travailler ensemble pour garantir le développement, le déploiement et l'utilisation responsables de l'intelligence artificielle dans le domaine militaire. Les applications militaires de l'intelligence artificielle génèrent à la fois des possibilités et des risques. L'Australie continuera de prendre une part active à ces travaux qui sont au cœur des nouvelles préoccupations de la communauté internationale, notamment lors du Sommet sur l'intelligence artificielle responsable dans le domaine militaire, qui se tiendra l'année prochaine en République de Corée. Nous saluons le rôle moteur joué par les États-Unis s'agissant de la déclaration politique sur l'utilisation militaire responsable de l'intelligence artificielle et de l'autonomie. L'Australie continuera de travailler avec diligence avec tous les États Membres pour parvenir à un consensus sur les questions liées à la cybernétique et à l'intelligence artificielle, sur la base d'un engagement en faveur du droit international et des normes de comportement responsable des États.

M. Vidal Mercado (Chili) (*parle en espagnol*) : Le Chili s'associe à la déclaration faite par le représentant de l'Indonésie au nom du Mouvement des pays non alignés.

Nous estimons non seulement que l'utilisation malveillante du numérique a des conséquences néfastes sur le développement et le bien-être des États, sur leurs niveaux de numérisation, de résilience et de développement des infrastructures, mais qu'elle représente aussi une menace pour la sécurité internationale. De même, les

cyberattaques et les activités malveillantes dans le cyberespace peuvent avoir des conséquences plus graves sur certains groupes et entités, tels que les personnes âgées, les personnes vulnérables, les femmes et les filles. La communauté internationale doit donc continuer à œuvrer pour dégager un consensus qui garantira que notre cyberespace reste libre, ouvert, accessible, stable, sûr et pacifique. Le Chili estime que le droit international, en particulier la Charte des Nations Unies, constitue le cadre normatif applicable qui doit régir le comportement responsable des États dans le cyberespace, y compris le droit international humanitaire, le droit international des droits humains et les 11 règles volontaires et non contraignantes de l'ONU.

Nous prenons acte des progrès accomplis dans le cadre du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), en particulier en ce qui concerne la création d'outils, le renforcement des capacités et l'élaboration de mesures de confiance. À cet égard, je souligne la création du répertoire mondial d'interlocuteurs. Nous tenons également à mettre en avant le programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. Nous devons être en mesure d'améliorer nos capacités et de créer des forums de coopération et d'échange d'informations, favorisant ainsi les travaux avec toutes les parties intéressées, telles que le secteur privé, la société civile, le monde universitaire et la communauté technique, entre autres. Nous soulignons également l'importance de resserrer les liens régionaux et de travailler avec les organisations régionales pour mettre en œuvre le cadre du groupe de travail à composition non limitée.

Il ne fait aucun doute que le désarmement, la non-prolifération et la maîtrise des armements peuvent avoir une incidence positive sur le bien-être humain, l'égalité et la justice, et en particulier sur le développement dans le monde entier, notamment dans les pays les moins avancés, les petits États insulaires en développement et les pays en développement sans littoral. Les sommes considérables consacrées aux dépenses militaires pourraient clairement être utilisées à meilleur escient. Nous devons promouvoir une plus grande représentation des pays les moins avancés dans les instances multilatérales qui débattent du désarmement et de la sécurité internationale.

Enfin, nous appelons tous les États Membres à soutenir les trois projets de résolution présentés par le Mouvement des pays non-alignés sur ce groupe de questions et sur d'autres, et nous soulignons également le projet de résolution A/C.1/78/L.19 sur les jeunes, le désarmement et la non-prolifération. Nous estimons que nous devons sensibiliser nos jeunes à ces questions urgentes afin que nos dirigeants et décideurs de demain soient informés et éduqués sur ces questions très sensibles, ce qui nous aidera à vivre en paix et à construire un monde meilleur. Nous tenons également à remercier la société civile, les établissements d'enseignement et les organisations non gouvernementales qui s'attachent à diffuser des informations sur le désarmement et la sécurité internationale.

M^me^ Hanlumyuang (Thaïlande) (*parle en anglais*) : La Thaïlande 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 (ASEAN).

La cybersécurité est l'une des questions les plus importantes dans le monde interconnecté d'aujourd'hui. L'utilisation abusive du numérique constitue de plus en plus une menace grave pour la paix et la sécurité internationales, ainsi que pour l'humanité. Il est impératif que nous nous efforcions de promouvoir un cyberespace ouvert, sûr, sécurisé, stable, accessible, interopérable, pacifique et résilient. Pour ce faire, la Thaïlande souhaite rappeler les quatre points importants suivants.

Premièrement, la Thaïlande réaffirme l'importance d'un cyberespace fondé sur des règles afin de prévenir les activités malveillantes et les conflits dans le cyberespace. Nous réaffirmons notre position de longue date : le droit international, en particulier la Charte des Nations Unies, est applicable dans le contexte du numérique. En complément du droit international, les 11 normes volontaires et non contraignantes de comportement responsable des États dans le cyberespace constituent une base très solide pour promouvoir la confiance entre les États. Il est essentiel que les États continuent de chercher à comprendre la manière dont le droit international s'applique au numérique et à recenser les lacunes à cet égard. Les États doivent collaborer pour élaborer des orientations supplémentaires, notamment une liste de contrôle sur la mise en œuvre des normes.

Deuxièmement, un dialogue institutionnel régulier qui soit ouvert, inclusif et transparent constitue un espace dont nous avons besoin pour débattre des questions susmentionnées. Ce dialogue pourrait également être l'occasion de mettre en commun les meilleures pratiques et d'améliorer les mesures de renforcement des capacités. L'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) demeure un cadre essentiel pour ce dialogue. Nous remercions l'Ambassadeur Burhan Gafoor, de Singapour, pour sa présidence exceptionnelle, qui a permis l'adoption par consensus du deuxième

rapport d'activité annuel (voir A/78/265). La Thaïlande se félicite de la proposition relative à la mise en place d'un futur mécanisme visant à promouvoir un dialogue institutionnel régulier sur ces questions, y compris le programme d'action. Nous sommes favorables à un mécanisme à voie unique, dirigé par les États, permanent et placé sous l'égide de l'ONU.

Troisièmement, la Thaïlande souligne le rôle essentiel des mesures de confiance dans la promotion de la confiance entre les États dans le cyberespace à tous les niveaux. La Thaïlande se félicite des résultats concrets obtenus par le groupe de travail s'agissant de l'élaboration et la mise en service d'un répertoire mondial et intergouvernemental d'interlocuteurs, qui pourrait faciliter des communications directes et sécurisées entre les États afin de prévenir et traiter les atteintes graves à la sécurité du numérique et de désamorcer les tensions dans des situations de crise. Il est tout aussi important de renforcer les mesures de confiance grâce à des efforts régionaux. Dans le cas de l'ASEAN, les initiatives et mécanismes régionaux liés aux mesures de confiance comprennent la stratégie de coopération en matière de cybersécurité pour la période 2021-2025, le comité de coordination de la cybersécurité et la réunion intersessions du Forum régional de l'ASEAN sur la sécurité des technologies de l'information et des communications et de leur utilisation.

Enfin, la Thaïlande est consciente que des programmes de renforcement des capacités sont nécessaires pour aider les États à améliorer leur cyberrésilience ainsi que la mise en œuvre des normes et du droit international. Nous encourageons les États en mesure de le faire à continuer de soutenir ces programmes, qui doivent être durables, politiquement neutres, transparents et axés sur la demande. À cet égard, nous tenons à remercier le Japon de son soutien continu au Centre de renforcement des capacités de cybersécurité de l'ASEAN-Japon à Bangkok depuis 2018.

En conclusion, la Thaïlande est déterminée à collaborer activement avec toutes les parties à la conciliation des points de vue divergents, afin de créer un environnement numérique plus sûr, sécurisé et stable.

M. Saadi (Iraq) (*parle en arabe*) : Tout d'abord, ma délégation s'associe aux déclarations faites par les représentants de la Jordanie, au nom du Groupe des États arabes, et de l'Indonésie, au nom du Mouvement des pays non alignés.

La délégation iraquienne se joint aux appels lancés à Israël pour qu'elle mette fin au bombardement brutal de civils non armés dans la bande de Gaza. Nous insistons sur la nécessité d'un cessez-le-feu et de l'acheminement de l'aide humanitaire pour mettre fin aux souffrances humanitaires et aux déplacements forcés systématiques de la population gazaouite.

La possession, la modernisation et l'augmentation continues des arsenaux militaires et la montée des tensions internationales et régionales se traduisent par une intensification de la course aux armements et des dépenses militaires mondiales, ce qui, collectivement, fait peser de graves menaces sur la paix et la sécurité internationales et régionales. C'est pourquoi nous devons tous prendre des mesures urgentes et concrètes pour réduire ces menaces et promouvoir la paix et la sécurité internationales et régionales afin d'atteindre les objectifs de développement durable d'ici à 2030.

La délégation iraquienne souligne que la promotion de l'universalité des conventions et traités de désarmement, y compris ceux relatifs à l'élimination des armes de destruction massive, en particulier les armes nucléaires, est la seule garantie du non-recours à la menace ou à l'emploi de ces armes et de la prévention de leurs répercussions catastrophiques. Ces armes sont létales et destructrices pour l'être humain comme pour l'environnement. Les solutions convenues par les Nations Unies 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.

La délégation iraquienne exprime sa préoccupation croissante face à l'augmentation des tensions internationales et régionales dans le contexte de la sécurité internationale. Cette situation a entraîné une utilisation accrue du numérique dans des activités qui menacent la paix et la sécurité régionales et internationales. À cet égard, l'Iraq se félicite de l'adoption du deuxième rapport d'activité annuel (voir A/78/265) du groupe de travail à composition non limitée créé en application de la résolution 75/240, adoptée en 2020, et salue également les efforts exceptionnels déployés par le Président du groupe de travail, l'Ambassadeur Burhan Gafoor. Nous sommes disposés à lui apporter tout notre soutien et à tout mettre en œuvre pour assurer le succès des sessions à venir afin d'adopter des recommandations qui bénéficient à tous les États, en particulier les États en développement, et les aident à relever les défis et à faire face aux risques découlant de l'utilisation du numérique, ainsi qu'aux menaces croissantes dans ce domaine. Cela contribuera à la création d'un cyberespace sûr, sécurisé et accessible à tous.

M. Ahmed (Pakistan) (*parle en anglais*) : Nous sommes à l'aube d'une étape majeure de l'histoire technologique de l'humanité, marquée par l'avènement de l'intelligence artificielle. L'évolution inévitable de l'intelligence artificielle, des algorithmes aux armements, se poursuit sans qu'aucune protection adéquate n'ait été mise en place s'agissant de sa conception, de son développement et de son utilisation. Nous sommes également au bord d'une nouvelle course aux armements, où les algorithmes seront aux commandes. Alors que l'intelligence artificielle se dirige vers le champ de bataille, il est raisonnable de se demander si les humains continueront d'en avoir la maîtrise, et dans quelle mesure, et s'ils pourront la désactiver.

En l'absence de contrôle humain, ces nouveaux moyens et capacités militaires fondés sur la technologie peuvent accroître les risques nucléaires, augmenter la probabilité d'erreurs d'appréciation et d'accidents et susciter des réactions asymétriques, abaissant ainsi le seuil de déclenchement de l'emploi de la force et des conflits armés. En temps de crise, il serait très déstabilisateur que le seuil de l'emploi de la force soit bas. Ces nouveaux outils sont également susceptibles de remodeler la dynamique des conflits, de modifier les stratégies de dissuasion, d'intensifier la course aux armements, d'introduire des schémas d'escalade imprévus et d'engendrer de nouveaux risques dans un contexte sécuritaire international déjà complexe.

Si certains États mettent en avant les avantages tirés de l'utilisation de l'intelligence artificielle sur le champ de bataille, il est tout aussi important de souligner les immenses risques et les conséquences potentiellement catastrophiques que cela comporte. Les possibilités d'agir et de mettre en place des garde-fous s'amenuisent rapidement alors même que nous nous approchons d'une percée technologique sur le champ de bataille. Si l'on ne parvient pas à traiter ces risques graves pour la paix et la sécurité, les États qui présentent des asymétries importantes seront contraints de se défendre avec les moyens dont ils disposent. Il est encourageant de constater le nombre croissant d'initiatives régionales et d'efforts multilatéraux visant à répondre aux appréhensions liées aux capacités militaires de l'intelligence artificielle. Nous appuyons également l'appel lancé par le Secrétaire général en faveur d'une gouvernance de l'intelligence artificielle.

La réponse du dispositif multilatéral est plutôt modeste et insuffisante à cet égard. Les débats tenus dans le cadre de la Convention sur certaines armes classiques portent principalement sur l'application du droit international humanitaire et ne visent qu'à traiter des questions relatives aux systèmes d'armes létaux autonomes. Ils n'abordent ni le thème plus large du développement de l'intelligence artificielle dans toutes les applications militaires fondées sur cette intelligence, y compris son intégration dans les domaines existants, ni ses conséquences sur la sécurité et la stabilité aux niveaux mondial et régional.

Pour la première fois, un groupe de pays a déposé, à la Première Commission, un projet de résolution (A/C.1/78/L.56) sur les systèmes d'armes létaux autonomes. Nous sommes d'avis que les discussions sur les systèmes d'armes létaux autonomes devraient se poursuivre au sein des groupes d'experts gouvernementaux créés au titre de la Convention sur certaines armes classiques dans le but d'élaborer des règles internationales au moyen d'un nouveau protocole. Parallèlement, d'autres organes de désarmement peuvent et doivent jouer un rôle complémentaire pour aborder la question plus large de l'intelligence artificielle dans les applications militaires, d'une manière qui crée des synergies positives tout en évitant les doubles emplois.

L'ampleur des défis qui découlent de l'utilisation de l'intelligence artificielle à des fins militaires, y compris dans les systèmes d'armes, nécessite une réponse globale multilatérale et multiforme. C'est pourquoi le Pakistan a présenté cette année un document de travail à la Conférence du désarmement, dans lequel il est proposé d'inscrire à l'ordre du jour un point relatif aux implications, pour la sécurité et la stabilité, des applications militaires de l'intelligence artificielle.

La militarisation du numérique et du cyberespace fait peser des menaces redoutables sur la paix, la sécurité et la stabilité, au niveau tant international que régional. Les différences particulières entre les domaines physique et cybernétique, ainsi que l'étendue et la portée de l'applicabilité du droit international en vigueur et de son interprétation, exigent que nous accélérions l'examen, l'élaboration et le développement de normes et de règles correspondantes régissant l'utilisation du cyberespace. Les délibérations en cours au sein du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) peuvent permettre de dégager des conceptions communes susceptibles de servir de base à de nouveaux efforts normatifs propres à empêcher que le cyberespace ne devienne un autre domaine de conflit.

Nous nous félicitons également d'être associés à la déclaration commune faite par le représentant de la Chine sur la coopération internationale touchant les utilisations pacifiques dans le contexte de la sécurité

internationale. Le droit de tous les États d'utiliser la science et la technologie à des fins pacifiques, conformément à leurs obligations internationales, doit être garanti de manière non discriminatoire et sans restrictions injustifiées. Les efforts visant à réglementer les matières et technologies à double usage doivent se poursuivre au sein de l'Organisation des Nations Unies, dans un cadre multilatéral et inclusif.

M. Moriko (Côte d'Ivoire) : Ma délégation souscrit à la déclaration faite par l'Indonésie au nom du Mouvement des pays non alignés, et apportera les observations suivantes à titre national.

Relativement récentes, les menaces sécuritaires liées aux technologies numériques n'en demeurent pas moins parmi les plus complexes et les plus alarmantes. En effet, les utilisations hostiles du cyberespace par des acteurs étatiques et non étatiques se multiplient et évoluent rapidement dans leurs formes et leurs manifestations, avec parfois de graves répercussions sur tous les aspects de la vie humaine. Il s'agit d'un phénomène sans limite spatiale qui met gravement en péril la paix et la stabilité mondiales et auquel il convient de remédier diligemment.

Transcendant les frontières, une réaction à ce défi qui vise une véritable efficience ne peut faire l'économie de son inscription dans un cadre international et multilatéral. Elle devrait, notamment, être axée sur la protection des infrastructures critiques et des infrastructures d'information critiques qui subissent des attaques de plus en plus sophistiquées, causes de perturbations majeures, de dommages financiers et de risque pour la vie même des personnes. Une attention singulière doit être réservée à l'encouragement des efforts régionaux visant à faciliter les échanges d'expériences et de bonnes pratiques, à l'image du Cyber Africa Forum dont l'édition 2023, tenue les 24 et 25 avril en Côte d'Ivoire, a été consacrée à la protection des infrastructures critiques contre les cybermenaces.

Il est également important d'œuvrer à empêcher l'usage de l'espace virtuel à des fins terroristes de propagande, de planification et de logistique, notamment par une application plus effective de l'appel de Christchurch visant à supprimer les contenus terroristes et extrémistes violents en ligne, dont mon pays est signataire depuis septembre 2019.

Par ailleurs, il est capital de renforcer le cadre de comportement responsable des États mis en place sous les auspices de l'ONU, par l'accentuation de notre engagement en faveur de l'approfondissement de la réflexion conduite au sein du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Les avancées enregistrées dans les délibérations au sein de ce groupe suscitent un optimisme légitime pour ma délégation qui, encore cette année, s'est associée au consensus autour du deuxième rapport à mi-parcours (voir A/78/265), fondé sur une approche dynamique et concrète, y compris pour les étapes à venir.

Ma délégation salue, en particulier, l'établissement d'un répertoire mondial et intergouvernemental d'interlocuteurs, dont le but est d'intensifier l'interaction et la coopération entre les États, aux fins d'accroître la transparence et la prévisibilité, contribuant ainsi à sauvegarder la paix et la sécurité internationales. Mon pays se félicite également de la poursuite des discussions sur la nécessité et les modalités de mise en place 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. La Côte d'Ivoire appuie fortement ce programme d'action qui, dans le prolongement du groupe de travail, aurait une vocation de mécanisme permanent, inclusif et orienté vers l'action, afin de correspondre à l'exigence d'adaptation continue des actions de la communauté internationale face à un défi sécuritaire en constante mutation.

Mon pays soutient particulièrement, dans ce programme d'action, le concept d'une approche renouvelée du renforcement capacitaire des États, notamment les plus vulnérables. Une démarche de cette nature aura assurément des effets bénéfiques sur l'aptitude de réaction aux incidents cybernétiques. Elle s'avère, de ce fait, indispensable pour améliorer le potentiel de mise en œuvre, par tous les États, du cadre de comportement responsable, dans l'optique de consolider sa portée et de construire un environnement numérique pacifique, fiable et résilient. C'est tout le sens du parrainage, apporté par ma délégation l'an dernier déjà, et renouvelé à cette session, de la résolution qui promeut ce mécanisme et de notre plaidoyer en faveur d'une issue favorable des discussions sur son établissement.

M^me^ González López (El Salvador) (*parle en espagnol*) : Les technologies de l'information et des communications sont des outils fondamentaux dans le monde d'aujourd'hui, mais leur utilisation incompatible avec les règles de comportement responsable des États dans le cyberespace et contraire au droit international, en particulier la Charte des Nations Unies, remet gravement en question la sécurité et la stabilité internationales.

El Salvador est pleinement conscient de l'utilisation croissante des moyens cybernétiques pour menacer les infrastructures critiques, les infrastructures d'information critiques et les chaînes d'approvisionnement

mondiales. Ces menaces exigent un débat sérieux sur la réglementation en matière de comportement responsable, l'applicabilité du droit international dans le cyberespace et des mesures visant à promouvoir la confiance, les capacités et le dialogue institutionnel. Un tel débat a lieu au sein du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), auquel mon pays participe de manière constructive. Nous estimons que le groupe accomplit un travail essentiel pour établir des conceptions communes et trouver des convergences dans le domaine du cyberespace.

Malgré les progrès réalisés par El Salvador dans les domaines de la cybernétique et du numérique, nous sommes favorables à ce que ces discussions progressent à l'avenir dans un cadre permanent et inclusif, sous les auspices de l'Organisation des Nations Unies. C'est pourquoi nous avons présenté les vues de notre pays et participé aux consultations afin de fournir des éléments sur la portée, la structure et le contenu d'un futur programme d'action sur le comportement responsable des États dans le cyberespace.

À la présente session, la Première Commission a entendu un nombre croissant de représentants évoquer les implications des technologies émergentes, en particulier de l'intelligence artificielle, sur la sécurité internationale. Mon pays s'est exprimé de façon catégorique dans les instances pertinentes sur les risques associés, par exemple, à l'intelligence artificielle générative et à l'apprentissage automatique, mais nous voyons aussi se profiler des possibilités significatives d'améliorer nos systèmes de cybersécurité grâce à l'utilisation de l'intelligence artificielle. Nous appelons à une approche de la cybersécurité fondée sur l'intelligence artificielle et non à une approche de l'intelligence artificielle fondée sur la cybersécurité.

Nous demandons instamment à réglementer et promouvoir l'utilisation de l'intelligence artificielle en fonction des risques, à entamer des débats approfondis sur les modèles de gouvernance de cette technologie, et à continuer d'analyser les menaces et problèmes potentiels ayant des implications pour la sécurité internationale. En outre, il convient de souligner que l'utilisation de l'intelligence artificielle dans le domaine de la sécurité va au-delà des systèmes d'armes autonomes et englobe une nouvelle dimension axée sur l'automatisation et pas seulement sur l'autonomie. Nous appelons à une prise en compte globale de l'intelligence artificielle, car la nature de cette technologie, ses applications et ses utilisations touchent tous les aspects de la vie humaine, même ceux qui ne sont pas directement liés à la sécurité. Cette dépendance technologique s'accentue rapidement et doit faire l'objet d'un débat de fond.

En Première Commission, El Salvador a abordé l'approche transversale des questions de genre comme un outil essentiel pour comprendre les expériences différentes des femmes et des hommes en matière de sécurité. Le cyberespace ne fait pas exception. Il est indéniable que la violence fondée sur le genre peut être aggravée par l'utilisation du numérique.

Enfin, El Salvador attache une grande importance à la participation de nombreux acteurs à ces processus. Les défis posés par le cyberespace exigent la collaboration active de la société civile, des organisations non gouvernementales, des organisations régionales, des milieux universitaires et de l'industrie. Nous demandons donc instamment aux États Membres de continuer à travailler en tant compte des contributions précieuses de ces acteurs à nos délibérations.

M. Muhith (Bangladesh) (*parle en anglais*) : Le Bangladesh s'associe à la déclaration faite par le représentant de l'Indonésie au nom du Mouvement des pays non alignés. Qu'il me soit permis de faire part de ma position à titre national.

Le contexte sécuritaire mondial en mutation rapide, sous l'effet de l'évolution constante des technologies, souligne indéniablement la nécessité d'adopter diverses mesures de désarmement qui dépassent les cadres conventionnels. Les progrès rapides de la technologie, en particulier dans les domaines de l'intelligence artificielle, des systèmes d'armes autonomes, de la biotechnologie et des cybercapacités, ont révolutionné non seulement notre vie quotidienne, mais aussi le contexte sécuritaire mondial. Ces innovations ont ouvert la voie à un potentiel illimité de progrès humain et de croissance économique. Cependant, elles ont également introduit de nouvelles dimensions de risque, qui exigent des solutions de désarmement innovantes.

Le Bangladesh est profondément préoccupé par le développement des capacités militaires reposant sur l'intelligence artificielle, ainsi que par l'émergence des technologies quantiques, en particulier celles liées aux systèmes d'armes, qui ont mis en évidence les insuffisances des cadres de gouvernance existants. Notre responsabilité première est de mettre l'intelligence artificielle au service de la paix, non pas au service des conflits. C'est pourquoi nous insistons sur le besoin urgent de cadres globaux pour régir efficacement l'intelligence artificielle et les technologies émergentes afin de garantir leur utilisation responsable, efficace et éthique.

Nous sommes fermement convaincus que 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 dans le 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. Le multilatéralisme est notre seul espoir de créer un environnement numérique libre, sûr, stable, accessible et pacifique, et nous soulignons que l'ONU doit jouer un rôle de premier plan dans l'élaboration de normes internationales applicables au cyberespace.

À cet égard, le Bangladesh considère que le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) constitue le mécanisme central et inclusif du système des Nations Unies. Nous réaffirmons notre engagement constructif en faveur du succès du groupe de travail et nous nous félicitons de l'adoption par consensus de ses deux rapports d'activité annuels consécutifs. Conformément au deuxième rapport d'activité annuel (voir A/78/265), nous soutenons la mise en place d'un mécanisme permanent à voie unique, dirigé par les États et placé sous l'égide de l'ONU. Nous soutenons également la mise en place d'un processus ouvert, inclusif, transparent, durable et flexible qui puisse répondre efficacement aux besoins évolutifs des pays en développement dans l'environnement dynamique du numérique.

Nous sommes d'avis que, en l'absence de structure normative acceptée au niveau mondial, les principes inscrits dans la Charte des Nations Unies et le droit international pertinent doivent s'appliquer au cyberespace afin de maintenir la paix et la stabilité. Au Bangladesh, nous investissons dans la promotion d'une solide culture de la cybersécurité, tant dans le Gouvernement que dans la société. Nous avons mis en place les cadres, politiques et stratégies nécessaires, y compris la récente loi sur la cybersécurité de 2023, 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 et la pertinence de ces normes juridiques pour le désarmement de zones telles que les fonds marins ou l'espace doivent faire l'objet de recherches et d'analyses plus poussées. L'éducation est fondamentale pour promouvoir la compréhension des conséquences humanitaires et économiques de l'armement. Le Bangladesh souligne l'importance de l'éducation dans le domaine du désarmement et de la non-prolifération. Nous apprécions le travail précieux réalisé par l'Institut des Nations Unies pour la recherche sur le désarmement et soulignons la nécessité de disposer de ressources accrues et prévisibles pour aider l'Institut à élargir et à gérer sa base de connaissances, dans l'intérêt de tous les États Membres.

Pour conclure, 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 pour garantir un monde plus sûr.

M. Eustathiou de los Santos (Uruguay) (*parle en espagnol*) : L'Uruguay partage les préoccupations de nombreux États Membres concernant l'augmentation des activités malveillantes dans le domaine du numérique, en particulier celles qui ont des conséquences sur la vulnérabilité des secteurs liés aux infrastructure critiques, aux soins de santé, à la sécurité et à la défense. Ces activités malveillantes constituent un problème réel et croissant qui nécessite une plus grande coopération entre les États et entre les secteurs public et privé afin de protéger l'intégrité, les fonctions et la disponibilité du cyberespace.

En Uruguay, nous nous employons à renforcer notre Centre national d'intervention en cas de défaillance informatique, en améliorant ses activités de surveillance et d'intervention, afin de réduire au minimum le temps nécessaire à la détection des défaillances et aux interventions correspondantes, de réduire les risques et de générer d'importantes économies pour le pays. Pour faire face à ces menaces réelles et potentielles, l'Uruguay estime qu'il est essentiel que nous continuions à œuvrer en faveur d'une coopération accrue et du renforcement des capacités, en gardant à l'esprit les différences entre les pays lorsque nous abordons l'utilisation malveillante du numérique. Nous sommes d'avis que l'objectif principal du renforcement des capacités est de garantir la participation sûre, efficace et significative de tous les États dans le cyberespace afin de tirer parti des possibilités de développement durable qu'offre celui-ci. Cela dit, les mécanismes de coopération, tels que les formes de coopération traditionnelle Nord-Sud, Sud-Sud et triangulaire, donneront lieu à des mesures particulières d'assistance technique pour le renforcement des capacités, y compris celles visant à mettre en œuvre les 11 normes de comportement responsable des États dans le cyberespace élaborées dans le cadre de l'ONU.

L'Uruguay réaffirme l'importance des échanges de bonnes pratiques nationales en matière de prévention des menaces numériques. Mon pays mène de tels échanges avec un certain nombre de pays de notre région par l'intermédiaire de notre organisme chargé du numérique. Nous reconnaissons également que l'ONU joue un rôle fondamental dans la mise en œuvre des mesures de renforcement des capacités et dans la promotion de leur mise en œuvre partout dans le monde, comme cela a été récemment souligné dans les rapports de consensus 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 (voir A/76/135) et du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) (voir A/78/265).

Les évolutions technologiques doivent aller de pair avec des institutions solides, un cadre qui reconnaisse les droits humains et un environnement juridiquement sûr et fiable. En tant que sociétés, nous avons non seulement des obligations communes, mais aussi des droits et des possibilités. La mise en œuvre conjointe d'un cadre normatif doit se faire de manière coordonnée, en tenant compte des avis de tous les États Membres et en se fondant sur une approche du cyberespace centrée sur l'être humain.

À cet égard, notre pays a proposé un programme complet et continu, le programme numérique de l'Uruguay, dans lequel nous examinons le cadre réglementaire et encourageons une plus grande sensibilisation à cet égard, en coopération avec tous les parties prenantes. De notre avis, la transformation numérique va de pair avec la sécurité juridique. C'est pourquoi nous encourageons les changements normatifs nécessaires pour tenir compte des progrès technologiques, en donnant la priorité à l'amélioration des procédures administratives, des mécanismes d'échange d'informations entre les entités publiques et privées et de la gestion numérique des entreprises.

Ma délégation estime que lorsque nous adoptons des cadres réglementaires, nous devons nous concentrer sur l'accessibilité, les droits d'auteur, les droits des consommateurs, la concurrence loyale, la protection des données, la sécurité, la transparence et le cyberespace, et promouvoir le respect des normes et conventions internationales pertinentes.

M^me^ Muigai (Kenya) (*parle en anglais*) : Le Kenya s'associe aux déclarations faites par le Nigéria, au nom du Groupe des États d'Afrique, et par l'Indonésie, au nom du Mouvement des pays non alignés. J'ajouterai quelques remarques supplémentaires à titre national.

Nous remercions le Représentant permanent de Singapour, Président du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), de l'exposé qu'il présentera prochainement. Nous saluons les progrès remarquables accomplis par le groupe de travail à composition non limitée sous sa direction et nous escomptons d'autres résultats concrets dans ce domaine crucial.

À l'ère numérique, l'influence omniprésente de la technologie façonne notre société mondiale de plus en plus interconnectée. De fait, l'ère numérique, qui progresse rapidement, redéfinit en conséquence notre perception de la sécurité et notre mode de vie, y compris notre conduite de la diplomatie. Trouver l'équilibre insaisissable entre l'innovation et la prévention des intentions malveillantes est primordial, mais il s'agit d'une entreprise herculéenne. En l'occurrence, cela exige un effort collectif mondial dans le cadre d'une approche multilatérale.

À cet égard, notre tâche principale est claire : définir les règles, normes et principes de comportement responsable des États pour notre sécurité et pour l'utilisation du numérique. Compte tenu de la rapidité des progrès technologiques, il est impératif et urgent de créer un environnement responsabilisé, où la cybersécurité soit garantie et où la collaboration numérique mondiale soit entretenue de manière responsable. Dans cette entreprise primordiale, nous devons prendre en considération les initiatives des États qui sont à l'origine d'innovations importantes et qui ont fait œuvre de pionniers en matière de sécurité numérique. Nous encourageons ces États à faire preuve de générosité et à partager les informations et meilleures pratiques pertinentes afin d'aider les autres pays à mettre au point leur propre infrastructure de cybersécurité.

L'ONU doit également aider en amont les nations à renforcer leurs capacités numériques et à lutter contre les répercussions de la révolution numérique, y compris l'utilisation abusive de l'intelligence artificielle, des mégadonnées et des médias sociaux. À cet égard, il convient de poursuivre et de renforcer la coopération et la coordination en matière de renforcement des capacités dans le cadre des organismes et organisations multipartites spécialisés existants, tels que le Forum mondial sur la cyber expertise. L'étude et la compréhension continues du contexte en constante évolution des cybermenaces revêtent également une importance

cruciale. Si nous saisissons les menaces existantes et potentielles dans le domaine de la sécurité de l'information, nous pouvons investir dans des mesures préventives et préemptives dans le cadre de la coopération, de la collaboration et de la coordination.

Dans ses efforts pour sécuriser son espace numérique, le Kenya a notamment créé l'équipe nationale d'intervention en cas de défaillance informatique, mis en place une infrastructure à clefs publiques nationale et, récemment, inauguré le comité de coordination national en matière d'informatique et de cybercriminalité, qui comprend les ministères et organismes compétents et dispose d'un secrétariat à part entière pour assurer l'application effective de ses décisions.

Pour conclure, la délégation kényane souligne que le dialogue institutionnel régulier que nous avons défini dans le cadre de notre mission est primordial pour garantir non seulement que la voix de chaque nation soit entendue, mais aussi que nous apprenions, agissions et grandissions collectivement. Notre objectif commun doit être de créer un espace numérique inclusif et sûr pour les générations présentes et futures.

M. Gusmão de Sousa (Timor-Leste) (*parle en anglais*) : État en développement, le Timor-Leste partage avec de nombreux États les avantages qu'offrent les technologies numériques, et les menaces qu'elles posent, pour l'édification de la nation et les processus de développement du pays, dont le maintien de la paix et de la sécurité, fondé sur le respect de la souveraineté nationale de tous les États Membres et sur l'application des règles relatives à l'utilisation pacifique du numérique, conformément à la Charte des Nations Unies.

La récente pandémie de maladie à coronavirus (COVID-19) nous a montré l'importance de disposer de ressources solides dans le domaine de la sécurité du numérique. Nous devons accorder une attention particulière aux besoins des pays en développement s'agissant de l'application des règles existantes et de leur développement à venir. Le développement croissant du numérique, ainsi que des menaces émergentes dans le cyberespace, causeront des dommages susceptibles de nuire à nos vies. Le Timor-Leste, État de petite taille, est convaincu que l'ONU joue un rôle important en tant qu'instance multilatérale, car elle nous offre un meilleur espace de dialogue entre toutes les parties pour surmonter les divisions entre les pays et s'assurer que tous peuvent effectivement jouir des avantages que recèle le numérique.

Le Timor-Leste, qui a récemment engagé sa transition numérique, reste préoccupé par la menace croissante que constituent les cyberattaques contre des infrastructures et infrastructures d'information critiques. Les États en développement demeurent confrontés à diverses difficultés pour répondre aux cybermenaces. Le Timor-Leste estime donc que la coordination et la coopération, ainsi que la mise en commun des meilleures pratiques dans le cadre d'instances bilatérales, régionales et multilatérales, appuieront et renforceront les structures nationales. À cet égard, nous sommes d'avis que les précédents Groupe d'experts gouvernementaux et groupe de travail à composition non limitée ont engagé des travaux complémentaires et servi d'instances dynamiques pour renforcer la coopération et dialoguer sur la question de la cybersécurité.

Nous saisissons également cette occasion pour saluer l'action de Singapour à la tête des travaux de l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), et nous souhaitons souligner son rôle central dans le débat sur le numérique et la paix et la sécurité internationales sous les auspices de l'ONU. Nous nous félicitons de l'adoption du rapport d'activité annuel de 2023 (voir A/78/265) et de la création du répertoire mondial d'interlocuteurs, pour lequel nous établissons actuellement nos procédures internes.

En ce qui concerne le futur mécanisme de dialogue institutionnel régulier, le Timor-Leste salue la proposition visant à élaborer un programme d'action sur la cybersécurité, que nous envisageons comme un cadre inclusif, ouvert, transparent et efficace, sous l'égide de l'ONU. Néanmoins, nous souhaitons souligner que le groupe de travail reste l'instance appropriée pour élaborer le programme d'action et le mettre en place, car il s'agit d'un mécanisme inclusif qui reflète les intérêts de tous les États. Nous sommes également d'avis que, pour que le programme d'action soit adopté par tous, il doit être axé sur les mesures de confiance, en particulier s'agissant de répondre aux besoins des pays en développement, notamment en matière de renforcement des capacités, afin de donner des moyens à tous et de renforcer l'application des normes établies, y compris en comblant les lacunes juridiques dans l'applicabilité du droit international au cyberespace. Nous souhaitons donc que les discussions sur les propositions se poursuivent, y compris concernant certains détails, tels que les questions d'organisation, en vue de nous préparer.

Nous soulignons la nécessité de renforcer la coopération multilatérale pour s'adapter à l'évolution rapide des conditions de sécurité, y compris les faits nouveaux intervenus dans le cyberespace. Nous estimons que les mesures de confiance sont des outils

essentiels pour promouvoir la confiance et prévenir les conflits. À cet égard, nous réaffirmons notre attachement aux mécanismes de désarmement et insistons sur une participation égale des femmes à ces mécanismes.

Nous souhaitons également nous associer à la déclaration faite par le représentant de l'Indonésie au nom du Mouvement des pays non alignés, et souligner l'importance de veiller à ce que l'utilisation du numérique soit pleinement conforme aux buts et principes inscrits dans la Charte des Nations Unies et le droit international. Le Timor-Leste attache une grande importance au respect du régime juridique international concernant le désarmement et la maîtrise des armements. Il importe d'appliquer ce régime au cyberespace pour maintenir la paix et la stabilité. Alors que notre gouvernement investit massivement dans la transition numérique, nous établissons actuellement les cadre, stratégie et politique requis pour le cyberespace. Dans cette optique, nous sollicitons la coopération de tous à nos efforts, en particulier au regard du renforcement de nos capacités.

Enfin, nous sommes d'avis que la collaboration avec les secteurs concernés, tels que le secteur privé, aidera les États, en particulier les pays en développement, à comprendre la nature des menaces et à coopérer pour faire face de manière adéquate à ces menaces, ce qui enrichira ce processus.

M^me^ Rodríguez Mancia (Guatemala) (*parle en espagnol*) : L'environnement international est empreint de menaces à la paix, d'actes fréquents contre la sécurité mondiale et de fléaux qui affectent les plus vulnérables de nos sociétés. Malgré cela, le développement du numérique progresse à pas de géant, appelant notre attention sur la nécessité d'améliorer notre compréhension et de renforcer nos capacités nationales et notre coopération dans le cyberespace. Le cyberespace est devenu un domaine critique pour les activités mondiales en raison de sa nature civile et du double usage auquel il se prête. Il a également été utilisé à plus d'une occasion par des groupes criminels et des terroristes. Il est donc essentiel de protéger le cyberespace en veillant au comportement responsable des États pour garantir la paix et la sécurité internationales.

Il est particulièrement inquiétant que certains États développent le numérique à des fins militaires, ce qui rend de plus en plus probable l'utilisation de ces technologies dans de futurs conflits entre États. Cette situation complexe exige la participation et la coopération de tous les secteurs de nos pays pour mettre en place les cadres techniques et juridiques nécessaires au renforcement du cyberespace aux échelles mondiale et nationale. C'est pourquoi mon pays croit fermement qu'il faut continuer à promouvoir le renforcement des capacités, élément essentiel de la coopération entre les États pour promouvoir des mesures de confiance dans le domaine de la sécurité du numérique. Je réaffirme l'importance d'une pleine transparence et d'un appui à l'échange d'informations et à la diffusion des bonnes pratiques aux niveaux sous-régional, régional et international.

Ma délégation souligne que l'applicabilité du droit international au comportement des États dans le cyberespace, les normes volontaires et non contraignantes de comportement des États en temps de paix et la mise en œuvre de mesures de confiance restent essentielles, tout comme la nécessité de mettre en évidence les lacunes des pays en matière de cybersécurité et de défense. Mon pays accorde un intérêt tout particulier aux mesures de renforcement des capacités visant à créer un cyberespace plus équitable, qui contribuera à maintenir un équilibre dans le contexte de la sécurité internationale.

Le Guatemala a adopté une stratégie nationale de cybersécurité, dont l'objectif principal est de renforcer les capacités du pays en créant l'environnement et les conditions nécessaires à la participation et à l'épanouissement des personnes dans le cyberespace, ainsi qu'à la garantie de leurs droits humains. En outre, au cours de l'année écoulée, le Guatemala a considérablement avancé dans l'élaboration d'une législation sur la cybersécurité. Mon pays a l'honneur d'être membre observateur de la Convention du Conseil de l'Europe sur la cybercriminalité, qui vise à lutter contre la criminalité numérique et sur Internet en harmonisant les législations nationales, en améliorant les techniques d'enquête et en promouvant la coopération entre les États.

C'est pourquoi nous nous félicitons de l'adoption par consensus du deuxième rapport d'activité annuel (voir A/78/265) du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Nous soulignons l'importance du projet de résolution A/C.1/78/L.60 visant à promouvoir un programme d'action pour faire progresser la mise en place d'un mécanisme permanent en matière de comportement responsable des États dans l'utilisation du numérique dans le contexte de la sécurité internationale, que le Guatemala soutient. À cet égard, nous prenons note des recommandations formulées par le Secrétaire général dans le Nouvel Agenda pour la paix, dans lequel il propose la mise en place d'un mécanisme multilatéral indépendant permettant d'amener les États qui feraient une utilisation malveillante du cyberespace à en répondre.

Enfin, nous rappelons à tous les États qu'ils doivent utiliser le numérique à des fins pacifiques et pour le bien-être de l'humanité, en favorisant le développement durable de tous les pays, quel que soit leur degré de développement scientifique et technologique.

M. Varem (Estonie) (*parle en anglais*) : L'Estonie s'associe à la déclaration faite au nom de l'Union européenne, en qualité d'observatrice. J'aimerais ajouter les observations suivantes à titre national.

La prévention et la gestion des menaces pour la paix et la sécurité internationales, y compris les menaces découlant de l'utilisation malveillante du cyberespace, sont de la plus haute importance pour l'Estonie. Les menaces liées à l'utilisation du numérique évoluent et s'intensifient, ce qui accentue les préoccupations en matière de sécurité nationale et internationale. Les cyberincidents malveillants peuvent avoir des effets dévastateurs sur les objectifs de développement économique et social et sur les infrastructures critiques, ainsi que des implications directes pour la stabilité internationale.

En particulier, l'invasion illégale et non provoquée de l'Ukraine par la Russie a montré comment les cyberopérations sont utilisées à l'appui des objectifs militaires et font désormais partie intégrante des opérations militaires. Dans le cadre de l'agression russe, les autorités centrales et locales, les infrastructures critiques, le secteur de la sécurité et de la défense et les entreprises privées du pays sont pris pour cible dans le cyberespace. Les cyberopérations malveillantes ont également des répercussions dangereuses, ce qui souligne le caractère transfrontière des cybermenaces.

L'Estonie condamne fermement ces cyberopérations malveillantes. Nous insistons sur le fait que le droit international, y compris la Charte des Nations Unies dans son intégralité, le droit international des droits humains et le droit international humanitaire, s'applique pleinement au comportement des États dans le cyberespace. Les États Membres de l'ONU doivent unir leurs forces pour renforcer l'ordre international fondé sur des règles et y adhérer également dans le cyberespace. Nous rappelons que lorsqu'ils utilisent le numérique d'une manière incompatible avec les obligations qui leur incombent en vertu du cadre de comportement responsable en la matière, les États compromettent la paix et la sécurité internationales, ainsi que la confiance et la stabilité entre les États.

L'Estonie apprécie grandement le travail du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et se félicite de l'accord trouvé sur le rapport d'activité annuel (voir A/78/265) en juillet. Malgré la situation géopolitique difficile, le rapport de consensus souligne que les États Membres sont de plus en plus désireux d'approfondir les discussions sur le cadre du comportement responsable des États. L'Estonie a trouvé que les délibérations sur les menaces, les normes, le droit international, le renforcement des capacités et le futur dialogue institutionnel étaient très utiles pour clarifier les perspectives nationales et régionales et pour renforcer les engagements mondiaux en matière de cybersécurité.

Les États Membres de l'Organisation ont appelé à maintes reprises à la mise en place d'un mécanisme permanent des Nations Unies chargé des questions cyber dans le contexte de la sécurité internationale. L'Estonie continue d'appuyer la mise en place d'un programme d'action inclusif, à voie unique et orienté vers l'action après l'expiration, en 2025, du mandat de l'actuel groupe de travail à composition non limitée, tel que défini dans la résolution 77/37. Nous nous réjouissons à la perspective des prochaines réunions du groupe de travail, qui donneront de nouvelles occasions de façonner collectivement le programme d'action.

Enfin, nous tenons à réaffirmer l'importance de tirer parti des compétences spécialisées de la communauté des parties prenantes. Nous saluons les possibilités de participation véritable, régulière et substantielle du secteur privé, de la société civile et du monde universitaire aux sessions du groupe de travail. L'Estonie invite les États et les autres parties prenantes à poursuivre des échanges constructifs afin de partager et d'écouter, et d'œuvrer au renforcement de la cyberrésilience mondiale.

M^me^ Nam (Nouvelle-Zélande) (*parle en anglais*) : La Nouvelle-Zélande est attachée à promouvoir le comportement responsable des États dans un cyberespace libre, ouvert, pacifique et sûr. Les progrès technologiques dans le cyberespace peuvent rendre le monde plus sûr et contribuer à un développement durable, à la prospérité et à la croissance économique. Dans le même temps, le cyberespace devient de plus en plus un vecteur de menaces nouvelles et émergentes incompatibles avec la paix et la sécurité internationales. Il s'agit notamment du déploiement de logiciels rançonneurs, du ciblage d'infrastructures critiques et de l'utilisation malveillante de la cyberactivité, qui sont de plus en plus répandus dans le contexte des conflits armés.

La Nouvelle-Zélande attache une grande importance au travail collectif en vue de relever ces défis et promouvoir un comportement responsable des États en

ligne. À cet égard, nous nous félicitons du consensus dégagé en ce qui concerne le deuxième rapport d'activité annuel (voir A/78/265) du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) à sa cinquième session de fond, en juillet.

La Nouvelle-Zélande note, comme elle et beaucoup d'autres l'ont déjà fait, que le cyberespace n'est pas un espace de non-droit et que le droit international s'applique en ligne comme hors ligne. La Nouvelle-Zélande a jugé encourageant de voir les États continuer à échanger leurs vues nationales sur l'application du droit international, notamment concernant l'applicabilité du droit international humanitaire et du droit international des droits humains. Nous réaffirmons notre position selon laquelle la Charte des Nations Unies dans son intégralité est applicable et essentielle au maintien de la paix, de la sécurité et de la stabilité dans le cyberespace, et que les États peuvent et doivent s'attendre à devoir répondre de toute cyberactivité malveillante contraire à la Charte et au droit international.

Nous saluons le programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. Nous continuons à faire de grand progrès au sein du groupe de travail à composition non limitée et nos discussions ont mis au jour de nombreuses questions que nous devons aborder collectivement. Nous constatons qu'un mécanisme permanent, inclusif, flexible et adaptable de dialogue institutionnel régulier sera nécessaire après la conclusion du mandat de l'actuel groupe de travail à composition non limitée afin de poursuivre la mise en œuvre du cadre de comportement responsable des États et faciliter encore les travaux sur une série de questions, en s'appuyant sur les résultats des groupes d'experts gouvernementaux et des groupes de travail à composition non limitée successifs.

Nous saluons et soutenons le projet de résolution A/C.1/78/L.60, présenté par la France, qui prévoit une voie claire et transparente permettant à tous les États Membres d'examiner la portée, la structure, le contenu et les modalités du futur mécanisme d'une manière complémentaire à l'actuel groupe de travail.

Enfin, nous rappelons également l'importance d'une participation multipartites, y compris de l'industrie, du monde universitaire et de la société civile, pour relever les nombreux défis posés par le cyberespace. Ces défis ne peuvent être relevés par les seuls gouvernements. Les parties prenantes non gouvernementales continuent d'apporter une perspective essentielle et des connaissances spécialisées précieuses aux discussions internationales sur la cybersécurité, et nous continuons à saluer et à encourager le dialogue avec toutes les parties prenantes.

M. Ogasawara (Japon) (*parle en anglais*) : Nous sommes témoins d'une menace croissante dans le cyberespace en raison de l'augmentation du nombre d'incidents impliquant l'utilisation malveillante des technologies de l'information et des communications, tels que les attaques de logiciels malveillants, les cyberopérations contre les infrastructures critiques et le vol de cryptomonnaie. Il n'y pas de frontières dans le cyberspace. C'est pourquoi la coopération internationale est une nécessité absolue pour nous tous.

Dans ce contexte, le Japon attache une grande importance au groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), instance centrale et inclusive sous les auspices de l'ONU. Nous saluons le rôle moteur de la présidence singapourienne et de son équipe et nous nous félicitons de l'adoption du deuxième rapport d'activité annuel (voir A/78/265) en juillet, ainsi que des progrès importants que nous avons réalisés collectivement, tels que la mise en place du répertoire mondial d'interlocuteurs.

Nous devons promouvoir l'état de droit dans le cyberespace. Le cyberespace n'est pas un espace de non-droit. Le droit international, notamment la Charte des Nations Unies et le droit international humanitaire, s'applique au cyberespace. Compte tenu de l'évolution rapide de la nature de l'environnement numérique, notre priorité doit être de mener de nouvelles discussions concrètes sur la manière dont le droit international s'applique à cet environnement. Nous attendons avec intérêt la tenue de discussions plus concrètes et plus substantielles sur ce sujet important, y compris dans le cadre des réunions intersessions du groupe de travail à composition non limitée.

Le renforcement des capacités est un autre domaine prioritaire. Le Japon collabore étroitement avec l'Association des nations de l'Asie du Sud-Est, la Banque mondiale et d'autres partenaires internationaux afin d'intensifier les efforts de renforcement des capacités régionales et mondiales dans le domaine du numérique. La table ronde mondiale sur le renforcement des capacités en matière de sécurité numérique, prévue en mai 2024 et à laquelle participeront de nombreuses parties prenantes, sera une excellente occasion pour tous les États Membres d'échanger leurs vues sur les mesures pratiques de renforcement des capacités.

En ce qui concerne le dialogue institutionnel régulier, nous remercions le groupe interrégional d'auteurs d'avoir présenté le projet de résolution A/C.1/78/L.60 concernant le programme d'action proposé par la France. Le Japon estime que cette proposition de programme d'action flexible, inclusif et à voie unique peut assurer une transition en douceur vers un nouveau mécanisme permanent et orienté vers l'action après 2025, où nous pourrons développer davantage les réalisations du groupe de travail à composition non limitée. Nous espérons sincèrement que le projet de résolution, fruit de nos efforts collectifs, sera adopté avec le large soutien des États Membres.

Seul pays à avoir subi des bombardements atomiques en temps de guerre, le Japon attache une importance primordiale à nos efforts en matière de désarmement et à l'éducation à la non-prolifération. En août dernier, lors de la dixième Conférence des Parties chargée d'examiner le Traité sur la non-prolifération des armes nucléaires, le Premier Ministre Fumio Kishida a annoncé la création du Fonds des jeunes leaders pour un monde exempt d'armes nucléaires, dans le cadre des efforts que nous déployons au titre du Plan d'action d'Hiroshima, qu'il a également présenté à cette même Conférence. Le principal objectif du Fonds est de permettre à de futurs leaders d'États dotés ou non dotés d'armes nucléaires de se rendre au Japon afin de constater sur place les réalités de l'emploi d'armes nucléaires. Il vise également à constituer un réseau mondial regroupant plusieurs générations de leaders et d'acteurs clefs représentant les gouvernements, la société civile, le milieu de l'éducation, le milieu universitaire, les médias, l'industrie et d'autres secteurs d'activité.

Les tragédies d'Hiroshima et de Nagasaki ne doivent jamais se répéter. La sensibilisation aux expériences vécues à Nagasaki et à Hiroshima après l'utilisation d'armes nucléaires doit sous-tendre nos efforts collectifs en faveur d'un monde exempt d'armes nucléaires. Le Japon considère qu'il est de son devoir de transmettre ces expériences aux générations futures et au-delà des frontières.

M. van der Haegen (Suisse) : Les cyberopérations malveillantes menées par des acteurs étatiques et non étatiques n'ont cessé d'augmenter ces dernières années, que ce soit en temps de paix ou lors de conflits armés. La guerre contre l'Ukraine illustre cette évolution et n'est pas la seule. Les cyberattaques menées par des acteurs criminels contre des entreprises ou des particuliers, contre des infrastructures critiques ou directement contre des États, comme l'a montré l'attaque contre le Costa Rica par exemple, sont en augmentation exponentielle. Ces défis ne peuvent être relevés que par le respect du cadre convenu en faveur d'un comportement responsable des États dans le cyberespace, tel qu'il a été confirmé et réaffirmé par les rapports consensuels des groupes d'experts gouvernementaux et des groupes de travail, et approuvé par tous les États à l'Assemblée générale.

La Suisse se félicite de l'adoption du deuxième rapport d'activité annuel (voir A/78/265) du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), car il constitue une base solide pour les travaux futurs du groupe. Nous nous réjouissons en particulier de l'opportunité de poursuivre la discussion sur l'application du droit international, y compris le droit international humanitaire, dans le cyberespace. Nous saluons également l'accent mis sur la protection des infrastructures critiques et des infrastructures de l'information essentielles, ainsi que de la recommandation de poursuivre les discussions sur ce sujet. Les récents cyberincidents et la situation géopolitique actuelle ont montré que la protection des infrastructures critiques, en particulier les installations médicales et de soins de santé, est de la plus haute importance. Dans ce contexte, la Suisse estime que le groupe de travail devrait se concentrer sur une meilleure compréhension, la promotion et la mise en œuvre des 11 normes volontaires existantes avant d'en élaborer de nouvelles.

Nous remercions le Président du groupe de travail d'avoir présenté à la Commission un projet de décision qui englobe l'approbation du rapport d'activité annuel et le calendrier des réunions proposé. La Suisse soutient pleinement le projet de décision et l'approche procédurale et pratique. Nous devons également souligner que la Suisse a de fortes réserves concernant le projet de résolution présenté par la Fédération de Russie sur cette question (A/C.1/78/L.11), car il semble redondant et ferait double emploi avec le texte présenté par le Président du groupe de travail. Le projet présenté par la Fédération de Russie soulève également des questions de fond, notamment parce qu'il ne s'appuie pas sur un langage consensuel, qu'il adopte une approche à la carte, qu'il ne fait pas référence au cadre consensuel et qu'il tente d'adapter le mandat du groupe de travail. Cela pourrait remettre en question les progrès importants réalisés jusqu'à présent par l'actuel groupe. Dans ces conditions, la Suisse ne serait pas en mesure de soutenir ce projet.

La Suisse soutient les discussions en cours sur l'établissement d'un programme d'action sur la cybersécurité au sein du groupe de travail. Nous pensons que ce programme d'action est le plus à même de devenir le nouveau dialogue institutionnel régulier une fois que l'actuel groupe de travail aura achevé ses travaux en

2025. C'est pourquoi nous avons coparrainé la résolution (A/C.1/78/L.60), présentée par la France, la Colombie, le Sénégal et les États-Unis d'Amérique, qui permettra aux membres de l'ONU de faire avancer cette discussion.

Avant de conclure, je voudrais également souligner les nombreux défis auxquels nous sommes confrontés à la lumière des progrès technologiques rapides. Les répercussions de l'intelligence artificielle, mais aussi d'autres domaines de la science et de la technologie, y compris les sciences de la vie, sont très présentes à la Première Commission de cette année. À l'avenir, ces développements devraient être au centre des préoccupations de la Commission et nous devrions veiller à ce qu'elle adopte une résolution qui relie les différents volets de la maîtrise des armements et du désarmement aux technologies émergentes et qui examine les synergies complexes de la science et de la technologie et leur impact sur la paix et la sécurité internationales.

M^me^ Page (Royaume-Uni) (*parle en anglais*) : Le Royaume-Uni est attaché à promouvoir un cyberespace libre, ouvert, pacifique et sûr qui renforce la sécurité collective et appuie le développement mondial. Cette entreprise requiert que tous les États honorent et appliquent les engagements existants convenus dans le cadre de l'ONU, à savoir le cadre pour un comportement responsable des États dans le cyberespace et l'applicabilité du droit international existant au cyberespace, y compris la Charte des Nations Unies dans son intégralité.

Malgré ces engagements, certains États continuent d'agir de manière irresponsable. La Russie recourt à des cyberopérations dans le cadre d'une longue campagne d'hostilité et de déstabilisation contre l'Ukraine. Ces attaques ont des effets tangibles sur le monde réel. Nous sommes profondément préoccupés par le fait que, dans le projet de résolution présenté par la Russie, celle-ci tente de réinterpréter ces accords consensuels dans son propre intérêt et, ce faisant, sape le cadre que nous avons collectivement construit dans cette enceinte.

Les modèles de cyberactivité malveillante continuent d'évoluer. Nous assistons à une recrudescence des attaques contre les institutions, les processus et les valeurs démocratiques du Royaume-Uni. Nous réagirons fermement aux actes hostiles contre nos infrastructures nationales critiques, notamment en renforçant nos défenses grâce à l'équipe spéciale de défense de la démocratie et aux nouveaux pouvoirs conférés par la loi sur la sécurité nationale adoptée par le Parlement.

Les répercussions des logiciels rançonneurs sur les infrastructures nationales critiques sont susceptibles de porter atteinte à la paix et à la sécurité internationales, et nous nous félicitons donc des références à ce sujet dans le deuxième rapport d'activité annuel (voir A/78/265) du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Cette année, le Royaume-Uni, en coordination avec ses partenaires internationaux, a sanctionné 18 cyberacteurs qui utilisaient des logiciels rançonneurs. Nous continuerons de faire en sorte que ceux qui nous nuisent en subissent les conséquences et que les acteurs malveillants répondent de leurs actes.

En outre, le Royaume-Uni est particulièrement préoccupé par l'utilisation irresponsable des cybercapacités avancées disponibles dans le commerce. Ce marché en expansion englobe une grande variété de produits et de services, y compris des logiciels espions commerciaux. Dans un cadre juridique national et international qui protège les droits humains, les cyberoutils commerciaux peuvent être utilisés de manière responsable par les membres des forces de l'ordre pour prévenir la grande criminalité et le terrorisme. Cependant, l'utilisation abusive de ces outils peut porter atteinte aux droits humains et menacer notre sécurité collective et la stabilité du cyberespace. Il s'agit d'un problème complexe qui nécessite la mobilisation de toute une série de secteurs. Le Royaume-Uni et la France collaborent étroitement à l'élaboration d'une réponse multipartite et nous attendons avec intérêt la poursuite de la coopération avec tous les États Membres sur ce point.

Le Royaume-Uni salue les travaux du groupe de travail à composition non limitée, notamment l'équilibre prudent atteint dans son rapport annuel de consensus. Nous sommes déterminés à jouer le rôle qui est le nôtre dans l'adoption d'un comportement responsable dans le cyberespace et à aider les autres à faire de même. Nous allons notamment investir 32 millions de livres sterling cette année pour financer nos activités de renforcement des capacités, et participerons aux débats constructifs visant à faire progresser la compréhension commune des États sur la manière dont le droit international, y compris le droit international humanitaire, s'applique au cyberespace.

Le Royaume-Uni appuie le projet de résolution A/C.1/78/L.60, présenté par la France, visant à établir un mécanisme permanent, orienté vers l'action et inclusif après la conclusion, en 2025, du mandat de l'actuel groupe de travail, mécanisme qui s'appuierait

sur des résultats consensuels, notamment ceux obtenus au sein du groupe de travail. Un tel mécanisme assurerait la continuité des discussions des États sur le numérique dans le contexte de la sécurité internationale et permettrait de mettre en œuvre le cadre de comportement responsable des États dans le cyberespace et de poursuivre son élaboration.

Pour terminer, je voudrais dire un mot sur les régimes multilatéraux de contrôle des exportations, 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. Nous sommes préoccupés par les efforts que certains États continuent de déployer pour saper et discréditer ces régimes essentiels.

M. Ghorbanpour Najafabadi (République islamique d'Iran) (*parle en anglais*) : La République islamique d'Iran présente ses condoléances les plus sincères à la nation palestinienne et lui témoigne sa ferme solidarité. Nous condamnons fermement les atrocités commises par le régime israélien à Gaza, qui ont jusqu'à présent coûté la vie à plus de 5 000 personnes, dont plus de 60 % sont des enfants et des femmes. Il faut immédiatement mettre fin à cette hécatombe et aux bombardements aveugles, et l'aide humanitaire doit être acheminée sans rencontrer d'obstacle.

Ma délégation s'associe à la déclaration faite par le représentant de l'Indonésie au nom du Mouvement des pays non alignés.

Face à la montée en flèche des cyberattaques, qui auraient augmenté de 50 % en 2022, la République islamique d'Iran réaffirme avec force sa position inébranlable sur l'utilisation du cyberespace et de l'environnement numérique. Nous sommes fermement convaincus que les atouts inestimables de cet environnement, comparables à un patrimoine commun de l'humanité, doivent être exploités exclusivement à des fins pacifiques, et qu'il est impératif que les États collaborent tout en respectant scrupuleusement le droit international applicable.

Conformément à cette position de principe, la République islamique d'Iran s'est engagée activement dans des négociations intergouvernementales tenues sous les auspices des Nations Unies. Notre participation est motivée par un attachement profond à sauvegarder les droits de toutes les parties concernées. Conformément à la résolution 75/240, par laquelle a été créé le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), le principe directeur de la méthodologie de travail du groupe de travail est le consensus. Cela implique de respecter les perspectives de chaque État Membre. L'essence du consensus doit être préservée et promue, car elle sous-tend les délibérations du groupe du travail.

Au vu de l'adoption du deuxième rapport annuel du groupe du travail (voir A/78/265), assorti d'un ensemble complet de déclarations clarifiant les vues des États Membres, y compris la République islamique d'Iran, nous percevons que la poursuite des progrès et le succès final du groupe de travail dépendent fondamentalement de l'obtention d'un consensus de fond. Comme nous l'avons souligné précédemment, la participation volontaire des États Membres au consensus ou la décision de ne pas y faire obstacle ne doit pas être considérée comme acquise. Dès lors, c'est à nous qu'il incombe de prendre en considération les points de vue et les contributions de tous les États Membres et de les intégrer avec diligence dans les rapports du groupe de travail.

Dans cette optique, il est essentiel que nous examinions les documents précédents du groupe de travail, y compris le résumé du Président et le rapport d'activité annuel de 2021 (voir A/77/275), qui recensent de manière substantielle les questions en suspens. Ces documents doivent servir de base à des négociations constructives et au rapprochement de vues divergentes. Nous souhaitons souligner que si nous aspirons à ce que le groupe de travail fonctionne efficacement en tant que mesure de confiance, nous devons veiller à prendre en compte les préoccupations et les intérêts de tous les États Membres. À défaut, la confiance essentielle dont jouit le groupe de travail s'en trouvera érodée. Cette confiance est inestimable pour la mission qu'il a à remplir.

Compte tenu de l'évolution des réalités, il est essentiel de reconnaître que certains États, notamment les États-Unis, se sont non seulement engagés dans la militarisation du cyberespace, mais ont aussi mené de nombreuses cyberattaques. Le régime israélien, en particulier, a lancé une série de cyberattaques contre la République islamique d'Iran, dont le fameux Stuxnet est un exemple frappant. Nous condamnons sans réserve ces actes et implorons la communauté internationale d'amener les responsables à répondre de leurs actes. Malheureusement, la République islamique d'Iran s'est récemment retrouvée impliquée, à tort et sans fondement, dans une prétendue cyberattaque. Nous rejetons catégoriquement toute allégation infondée reposant sur des affabulations et mettons en garde contre ce type d'allégations.

M. Getahun (Éthiopie) (*parle en anglais*) : Ma délégation s'associe aux déclarations faites au nom du Mouvement des pays non alignés et au nom du Groupe des États d'Afrique.

La contribution du numérique à la paix, à la croissance et au développement est considérable et notoire. Pour que cette contribution ait des effets positifs et durables, il est extrêmement important de défendre les principes de comportement responsable des États dans l'utilisation du numérique à des fins exclusivement pacifiques. L'utilisation du numérique dans l'industrie augmente, mais les menaces liées à l'utilisation de ces outils à des fins criminelles augmentent elles aussi. Nous sommes d'avis que cela nuit à nos efforts collectifs visant à utiliser ces technologies pour garantir la paix et la stabilité et réaliser nos stratégies, et il faut donc y remédier rapidement.

L'Éthiopie œuvre avec d'autres au succès du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), qui est actuellement le seul mécanisme inclusif dans le cadre de l'Organisation des Nations Unies. La participation égale de tous les États à des résultats fondés sur le consensus est essentielle à sa réussite. À cet égard, l'Éthiopie souscrit au point de vue selon lequel un processus dirigé par les États et faisant rapport à la Première Commission constitue la meilleure approche. Dans le même ordre d'idées, nous sommes convaincus que les instances régionales sont également importantes pour parvenir au consensus dont nous avons besoin. Nous sommes donc d'avis que l'évolution de l'utilisation du cyberespace dans le contexte de la sécurité internationale pourrait faire l'objet d'un débat inductif, des niveaux sous-régional et continental jusqu'au niveau mondial, ce qui contribuerait à instaurer la confiance à tous les niveaux.

Nous insistons sur le fait que les pays en développement ont besoin de programmes de renforcement des capacités dans les domaines technique et juridique ainsi que dans les domaines du numérique qui sont importants en vue d'une utilisation pacifique du cyberespace. À cet égard, il est essentiel que le système des Nations Unies et les organisations régionales jouent un rôle clef pour appuyer le renforcement des capacités afin de permettre aux pays en développement d'améliorer leurs capacités à tous les niveaux et de tirer parti du numérique pour atteindre leurs objectifs de développement. Le soutien au renforcement des capacités est également essentiel pour les mesures de confiance, en vue de renforcer la stabilité et la sécurité du cyberespace.

L'Éthiopie travaille activement à l'utilisation des capacités numériques pour favoriser des changements économiques et sociaux rapides et construire une société plus prospère. Nous avons formulé des politiques et une législation visant à promouvoir le numérique et à tirer parti de son utilisation et nous avons progressé dans le renforcement des institutions afin d'exploiter le potentiel qu'offre le numérique et d'atteindre nos objectifs de développement. L'Éthiopie est attachée à contribuer à la mise en œuvre du Pacte numérique mondial, qui resserrera la coopération numérique dans le cadre d'un processus ouvert et inclusif, et à en retirer des avantages. Nous soutenons pleinement la promotion de solutions numériques par l'accès aux biens publics numériques et l'utilisation de ceux-ci afin d'atteindre les objectifs de développement durable et d'œuvrer à la réduction de la fracture numérique.

Dans le cadre de nos efforts visant à développer l'industrie numérique et à traiter efficacement les problèmes liés au cyberespace, nous avons rencontré plusieurs difficultés, notamment le manque de ressources financières et le faible niveau des compétences numériques et des compétences nécessaires à l'utilisation des biens publics numériques. Dans notre quête d'une utilisation efficace et durable du numérique afin de surmonter les multiples difficultés auxquelles nous sommes confrontés en matière de développement, nous demandons donc à la communauté internationale de fournir un appui axé sur la demande pour nous permettre d'éliminer les goulets d'étranglement qui entourent l'utilisation du numérique.

Pour conclure, l'Éthiopie souligne l'importance de garantir la paix, la sécurité et la stabilité de l'environnement numérique, et réaffirme son engagement à œuvrer de concert pour atteindre cet objectif.

M. Bérard Cadieux (Canada) (*parle en anglais*) : Le Canada souhaite aborder deux enjeux qui ont une incidence sur la paix et la sécurité internationales : le comportement responsable des États dans le cyberespace et l'importance que la prise en compte des questions de genre en matière de désarmement soit la règle, et non l'exception.

Le Canada se félicite du cadre cumulatif et évolutif de comportement responsable des États dans l'utilisation des technologies de l'information et des communications (TIC), élaboré dans le rapport de consensus (voir A/76/135) 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, ainsi que dans les rapports d'activité annuels de 2022 et 2023 (voir A/77/275 et A/78/265) du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

Ce cadre est essentiel pour la paix et la sécurité et pour parvenir à une compréhension commune de la manière dont les États doivent se comporter dans le cyberespace. Nous sommes donc préoccupés par le fait qu'un petit nombre d'États, dont certains ont joué un rôle notable dans son élaboration, remettent aujourd'hui en question la solidité de ce cadre. Nous rappelons que, dans les rapports du Groupe d'experts gouvernementaux de 2015 (voir A/70/174) et de 2021, la communauté internationale est convenue par consensus d'un ensemble de normes exhaustives et volontaires sur le comportement responsable des États dans le cyberespace, et que les États ont également convenu que le droit international s'appliquait dans le cyberespace. Ces normes et le droit international sont des moyens appropriés pour orienter les États quant à ce qu'ils peuvent et ne peuvent pas faire dans le cyberespace. Nous nous félicitons des discussions en cours au sein du groupe de travail à composition non limitée sur la mise en œuvre des normes et sur la manière dont le droit international s'applique.

Les actions concrètes pour renforcer les mesures de confiance et le renforcement des capacités sont deux autres éléments clefs du cadre pour un comportement responsable des États dans le cyberespace. Depuis 2015, le Canada a engagé dans le monde entier plus de 30 millions de dollars dans des projets de renforcement des capacités touchant le cyberespace, et il collabore avec diverses organisations pour promouvoir un Internet ouvert et sûr. Nous reconnaissons qu'il reste beaucoup à faire et nous nous réjouissons à la perspective d'approfondir nos discussions dans les années à venir.

(*l'orateur poursuit en français*)

Le Canada estime que les membres de l'ONU doivent instaurer un forum permanent en vue de favoriser les discussions pragmatiques à l'issue du mandat actuel du groupe de travail. C'est pourquoi le Canada est coparrain de la proposition du programme d'action lors de la Première Commission de cette année. Le programme d'action s'avère le meilleur forum pour faire progresser concrètement la mise en œuvre du cadre normatif convenu, notamment en soutenant des activités ciblées de renforcement des capacités. Le programme d'action offrira également à tous les États membres un forum inclusif leur permettant de se pencher sur ces questions et sur toutes les questions liées à la cybersécurité, tout en bénéficiant de l'expertise du secteur privé, de la société civile et du milieu universitaire.

Dans un souci d'inclusion, le Canada réaffirme que pour garantir un Internet ouvert, il faut investir dans l'égalité entre les genres et comprendre l'incidence sexospécifique des enjeux en matière de cybersécurité. Nous reconnaissons le travail effectué au sein du groupe de travail pour souligner les diverses contributions des femmes, la mise en place de documents sur le portail du groupe de travail et le programme de bourses « Femmes dans le domaine de la cybersécurité » en cours. Nous sommes impatients de nous appuyer sur ce programme lors des prochains travaux des Nations Unies en matière de cyberespace.

Les perspectives de genre sont essentielles dans le cyberespace, mais elles le sont tout autant dans l'ensemble des activités du mécanisme de désarmement. L'intégration du genre facilite la création d'initiatives efficaces et durables qui contribueront à intervenir face aux menaces de sécurité les plus pressantes dans le monde. L'un des moyens d'y parvenir est de recueillir et de partager des données ventilées par âge et par genre sur l'impact des armes. Le Canada est encouragé par l'augmentation de la représentation des genres dans les forums des Nations Unies, y compris au sein de la Première Commission. Cependant, le déséquilibre entre les genres demeure et nous omettons donc des voix et des points de vue primordiaux à la table : des voix et des points de vue qui sont nécessaires à l'élaboration de politiques et de programmes de non-prolifération et de désarmement plus efficaces.

En conclusion, il est nécessaire de combler le fossé entre les genres afin de créer un monde plus inclusif, pacifique et prospère. Le Canada reste donc ferme dans son engagement à travailler avec tous les intervenants afin de préconiser les considérations liées au genre dans tous les aspects de la sécurité internationale.

M. Shen Jian (Chine) (*parle en chinois*) : L'environnement international du cyberespace est actuellement complexe, critique et caractérisé par la formation de blocs, la militarisation et la fragmentation. Cette année marque le vingt-cinquième anniversaire du lancement du processus de sécurité des technologies de l'information et des communications (TIC) à l'Organisation des Nations Unies. Des groupes d'experts gouvernementaux au groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), ce processus onusien est parti de zéro et a pris de l'ampleur, avec des

réalisations importantes, notamment la confirmation des principes de souveraineté et de maintien de la paix dans le cyberespace, l'élaboration de 11 normes de comportement responsable des États dans le cyberespace, l'engagement à respecter et à appliquer le cadre de comportement responsable des États et la création récente du répertoire mondial et intergouvernemental d'interlocuteurs. Ces avancées durement acquises ont joué un rôle important dans le maintien de la paix et de la stabilité dans le cyberespace.

Les expériences réussies de ces 25 dernières années ont démontré que la seule façon de surmonter les difficultés, de se développer ensemble et de parvenir à la prospérité commune est de défendre la paix, la coopération et l'inclusion tout en rejetant les conflits, la confrontation et l'exclusivité. Le maintien du caractère pacifique du cyberespace est notre seule option. Nous devons placer la paix et la coopération au centre de nos politiques et démontrer notre volonté de rechercher la paix et le développement par la coopération, de rejeter les cyberconflits et la cyberguerre, et de permettre au cyberespace d'être un lieu riche en possibilités numériques plutôt qu'un nouveau champ de bataille pour les rivalités entre grandes puissances.

La gouvernance mondiale du cyberespace requiert la participation égale et la prise de décision conjointe de tous les pays. Nous devons soutenir fermement le rôle central que joue l'ONU dans les questions de sécurité de l'information, respecter l'autorité du groupe de travail à composition non limitée, seul processus consacré à la sécurité de l'information placé sous les auspices de l'Organisation, et unir nos efforts pour prendre des dispositions à long terme en faveur de la future instance chargée de la sécurité de l'information.

À l'ère numérique, nous devons prendre l'initiative de relever les nouveaux défis de la sécurité de l'information et travailler sans relâche sur les problèmes réels et urgents qui touchent tous les pays. Dans son deuxième rapport d'activité annuel, le groupe de travail à composition non limitée constate que :

> « Compte tenu de l'augmentation du volume de données associées aux technologies nouvelles et émergentes et de leur agrégation, les États ont également noté qu'il importait de plus en plus de protéger et de sécuriser les données » (*A/78/265, annexe, para. 17*).

La Chine a proposé une initiative mondiale sur la sécurité des données qui apporte une solution efficace à la sécurité des données au niveau mondial. Cette proposition pourrait servir de base à nos discussions futures. Face aux risques et aux défis du cyberespace, la Chine souhaite travailler avec toutes les parties, maintenir la solidarité et la coopération, et déployer des efforts conjoints pour construire une communauté d'avenir partagé dans le cyberespace.

L'intelligence artificielle est un nouveau domaine du développement humain qui a créé des possibilités considérables pour le développement socioéconomique, mais qui s'accompagne également de risques et de défis imprévisibles. La gouvernance de l'intelligence artificielle, tâche qui incombe à l'ensemble de la communauté internationale, intéresse l'avenir de l'humanité. Récemment, la Chine a lancé l'Initiative mondiale pour la gouvernance de l'intelligence artificielle, qui appelle tous les pays à renforcer leurs échanges et leur coopération et à travailler ensemble pour prévenir les risques. Nous devons élaborer des cadres de gouvernance de l'intelligence artificielle qui soient fondés sur un large consensus, afin de rendre les technologies de l'intelligence artificielle plus sûres, plus fiables, plus contrôlables et plus équitables. Auparavant, la Chine avait également publié des documents de position sur la réglementation des applications militaires de l'intelligence artificielle et sur le renforcement de la gouvernance éthique de l'intelligence artificielle.

La Chine préconise une approche centrée sur les personnes et des visions telles que l'intelligence artificielle au service du bien, en mettant l'accent en premier lieu sur le développement et l'éthique. Nous pensons que le développement de l'intelligence artificielle doit être systématiquement mis au service de la société. Nous devons travailler ensemble pour prévenir et combattre l'utilisation abusive et malveillante des technologies de l'intelligence artificielle par des terroristes, des extrémistes et des groupes criminels organisés transnationaux. Tous les pays, en particulier les grands pays, doivent adopter une approche prudente et responsable de la recherche, du développement et de l'application des technologies de l'intelligence artificielle dans le domaine militaire et s'abstenir de rechercher un avantage militaire absolu et de mettre en péril l'équilibre stratégique et la stabilité au niveau mondial.

La Chine préconise l'application d'une réglementation par niveau et par catégorie afin de garantir que les systèmes d'armes concernés sont toujours sous le contrôle de l'humain. Compte tenu de la nature à double usage de la technologie de l'intelligence artificielle, nous devons, tout en renforçant la réglementation et la gouvernance, garantir les droits de tous les pays à

leurs utilisations pacifiques. La Chine rejette les lignes idéologiques ou la formation de groupes exclusifs qui empêcheraient d'autres pays de développer leur intelligence artificielle. Nous sommes également contre le fait de dresser des obstacles et de perturber la chaîne d'approvisionnement mondiale de l'intelligence artificielle au moyen de monopoles technologiques et de mesures coercitives unilatérales.

La Chine soutient activement les discussions visant à établir une instance internationale chargée de la gouvernance de l'intelligence artificielle dans le cadre de l'ONU et à coordonner les efforts pour traiter les questions majeures concernant le développement, la sécurité et la gouvernance de l'intelligence artificielle.

M. Christoglou (Grèce) (*parle en anglais*) : La Grèce s'associe pleinement à la déclaration faite par le représentant de l'Union européenne, en qualité d'observatrice, et souhaite formuler quelques commentaires à titre national.

Les comportements malveillants dans le cyberespace se sont intensifiés ces dernières années, avec notamment une augmentation importante des cyberattaques visant les infrastructures critiques, les chaînes d'approvisionnement et la propriété intellectuelle, ainsi qu'une hausse des attaques par rançongiciels contre les entreprises, les organisations et les citoyens. Les cyberattaques sont également devenues un moyen de conflit armé, s'imposant comme l'une des plus importantes menaces de notre époque pour la paix et la sécurité. Dans cet esprit, la Grèce soutient fermement le travail accompli à l'Organisation, qui a notamment permis d'aborder la question de l'application du droit national dans le cyberespace. Des normes de comportement responsable et des mesures de confiance ont aussi été établies dans ce cadre. S'appuyer sur ces travaux contribue à faire progresser la paix et la stabilité dans le cyberespace et profite à tous les pays.

La Grèce se félicite également du rapport d'activité annuel de 2023 (voir A/78/265) adopté par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), et plus particulièrement de la recommandation invitant les États à engager des discussions sur la portée, la structure et le contenu d'un programme d'action visant à promouvoir un comportement responsable des États dans le cyberespace. Nous sommes fermement convaincus que la mise en place d'un mécanisme permanent, inclusif et orienté vers l'action constituerait une base solide pour la poursuite des deux aspects les plus importants de nos travaux : la mise en œuvre et la poursuite de l'élaboration du cadre de comportement responsable des États dans le cyberespace.

La Grèce est pleinement disposée à poursuivre à l'ONU les discussions sur les questions de cybersécurité et réaffirme sa volonté de travailler constructivement pour progresser, comme en témoigne sa participation active au processus du groupe de travail à composition non limitée depuis sa création.

La séance est levée à 12 h 55.