Nations Unies S/2021/621

Conseil de sécurité

Distr. générale
1er juillet 2021
Français
Original : anglais

Lettre datée du 1er juillet 2021, adressée au Secrétaire général et aux représentantes et représentants permanents des membres du Conseil de sécurité par le Président du Conseil de sécurité

J'ai l'honneur de vous faire parvenir ci-joint le texte de l'exposé de Mme Izumi Nakamitsu, Haute-Représentante pour les affaires de désarmement, et celui des déclarations faites par Mme Kaja Kallas, Première Ministre de l'Estonie, M. Mahamadou Ouhoumoudou, Premier Ministre du Niger, M. Simon Coveney, Ministre des affaires étrangères et de la défense de l'Irlande, M. Bui Thanh Son, Ministre des affaires étrangères du Viet Nam, M. Joe Mucheru, Secrétaire du Gouvernement chargé des technologies de l'information et des communications, de l'innovation et de la jeunesse du Kenya, Mme Linda Thomas-Greenfield, Représentante permanente des États-Unis et membre du Cabinet du Président Biden, M. Harsh Vardhan Shringla, Ministre des affaires étrangères de l'Inde, Mme Keisal M. Peters, Ministre d'État chargée des affaires étrangères et du commerce extérieur de Saint-Vincent-et-les Grenadines, M. Audun Halvorsen, Vice-Ministre des affaires étrangères de la Norvège, M. Tariq Ahmad de Wimbledon, Ministre d'État chargé du Commonwealth, de l'Organisation des Nations Unies et de l'Asie du Sud du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, et M. Franck Riester, Ministre délégué auprès du Ministre de l'Europe et des affaires étrangères, chargé du commerce extérieur et de l'attractivité de la France, ainsi que par les représentants de la Chine, de la Fédération de Russie, du Mexique et de la Tunisie, à l'occasion de la vidéoconférence consacrée au thème « Maintien de la paix et de la sécurité internationales : cybersécurité » et tenue le mardi 29 juin 2021.

Conformément à l'accord auquel sont parvenus les membres du Conseil pour cette visioconférence, les délégations et entités suivantes ont soumis des déclarations écrites, dont le texte est également joint : Afrique du Sud, Argentine, Allemagne, Australie, Autriche, Bahreïn, Belgique, Brésil, Canada, Chili, Comité international de la Croix-Rouge, Danemark, Égypte, El Salvador, Émirats arabes unis, Équateur, Géorgie, Grèce, Guatemala, Indonésie, Italie, Japon, Kazakhstan, Lettonie, Liechtenstein, Malte, Maroc, Nouvelle-Zélande, Organisation internationale de police criminelle, Pakistan, Pays-Bas, Pérou, Pologne, Qatar, République de Corée, République islamique d'Iran, Roumanie, Sénégal, Singapour, Slovaquie, Slovénie, Suisse, Thaïlande, Tchéquie, Turquie, Ukraine et Union européenne.

Conformément à la procédure énoncée dans la lettre du 7 mai 2020, adressée aux représentantes et représentants permanents des membres du Conseil de sécurité par le Président du Conseil (S/2020/372), qui a été arrêtée en raison de la situation exceptionnelle résultant la pandémie de maladie à coronavirus (COVID-19), le texte

de l’exposé et des déclarations sera publié comme document officiel du Conseil de sécurité.

(*Signé*) Nicolas **de Rivière**
Président du Conseil de sécurité

Annexe I

Déclaration de la Haute-Représentante pour les affaires de désarmement, M^me^ Izumi Nakamitsu

Je tiens à remercier l'Estonie d'avoir organisé cette réunion et de m'avoir invité à présenter un exposé lors de ce débat public sur le maintien de la paix et de la sécurité internationales dans le cyberespace.

En janvier de cette année, on comptait plus de 4,6 milliards d'utilisateurs actifs de l'Internet dans le monde. On estime qu'à l'échéance de 2022, 28,5 milliards d'appareils en réseau seront connectés à l'Internet, soit une augmentation considérable par rapport aux 18 milliards recensés en 2017.

À un moment où les progrès des technologies numériques continuent de révolutionner la vie humaine, nous devons rester vigilants quant à l'utilisation malveillante de ces technologies qui pourrait mettre en péril la sécurité des générations futures.

Les technologies numériques mettent de plus en plus à rude épreuve les normes juridiques, humanitaires et éthiques en vigueur, ou encore la non-prolifération, la stabilité internationale et la paix et la sécurité.

Elles facilitent les accès, entrouvrent de nouveaux domaines potentiels de conflit et offrent aux acteurs étatiques et non étatiques la possibilité de se livrer à des attaques, même au-delà des frontières des pays.

En ce qui concerne plus particulièrement les technologies de l'information et des communications (TIC), nous avons constaté, ces dernières années, une augmentation spectaculaire de la fréquence des actes malveillants. Ces actions, qui ont pris différentes formes, allant de la désinformation à la perturbation de réseaux informatiques, contribuent à saper la confiance entre les États.

Ces évolutions présentent également un risque particulier pour les infrastructures critiques tributaires des TIC, comme le secteur financier, les réseaux électriques et les installations nucléaires. Le Secrétaire général a appelé l'attention sur les cyberattaques menées contre des établissements de soins de santé pendant la pandémie, appelant la communauté internationale à faire davantage pour prévenir et éliminer ces nouvelles formes d'agression, qui peuvent causer d'autres préjudices graves aux civils[1].

Ces menaces liées aux TIC ont également des répercussions différenciées selon les sexes et doivent être analysées sous cet angle. L'extrémisme violent et le trafic en ligne ont des répercussions différenciées, souvent méconnues, sur les femmes, les hommes et les enfants, tout comme d'autres menaces liées aux TIC, telles que le cyberharcèlement, la violence au sein du couple et la diffusion non consentie d'informations et d'images intimes. C'est également la raison pour laquelle nous devons tout mettre en œuvre pour garantir la participation égale, pleine et effective des femmes et des hommes à la prise de décision dans le domaine numérique.

Si les menaces liées aux TIC augmentent, des initiatives sont également prises pour y faire face. À l'ONU, cinq groupes d'experts gouvernementaux ont étudié, durant les quinze dernières années, les menaces existantes et émergentes des TIC pour la sécurité internationale et ont recommandé des mesures pour y faire face. Deux autres processus relevant de l'ONU – un Groupe de travail à composition non limitée et un sixième Groupe d'experts gouvernementaux, tous deux établis en 2018 – ont

[1] Voir www.un.org/sg/en/content/sg/statement/2020-05-27/secretary-generals-remarks-the-security-council-open-debate-the-protection-of-civilians-armed-conflict-delivered.

récemment mené à bien leurs travaux respectifs et franchi d'importantes étapes dans ce domaine en adoptant des recommandations concrètes, orientées vers l'action.

Ces deux groupes ont défini un ensemble de normes d'application volontaire et non contraignantes relatives au comportement responsable des États, en donnant acte du fait que des normes supplémentaires pourraient être élaborées au fil du temps. Ils ont par ailleurs réaffirmé que le droit international, en particulier la Charte des Nations Unies, était applicable et essentiel au maintien de la paix, de la sécurité et de la stabilité dans l'environnement des TIC. Les groupes ont recommandé l'adoption de mesures de confiance, de renforcement des capacités et de coopération, qui s'appuieraient sur les travaux des processus précédents. Conformément à son mandat, le Groupe de travail à composition non limitée a en outre formulé des conclusions et des recommandations relatives à l'établissement d'un dialogue institutionnel régulier sur la question des TIC.

Comme l'a noté dans son rapport le Groupe d'experts gouvernementaux le plus récent, les mesures recommandées par les précédents Groupes d'experts gouvernementaux et le Groupe de travail à composition non limitée constituent ensemble un premier cadre de comportement responsable des États en matière d''utilisation des TIC[2].

Un deuxième Groupe de travail à composition non limitée vient également de tenir sa session d'organisation et commencera ses travaux de fond dans le courant de l'année.

À l'échelon régional, des organisations à caractère régional prennent désormais des initiatives importantes en ce qui concerne les questions relatives aux TIC. Les démarches à caractère régional ont pris diverses formes, déterminées par des priorités et des besoins différents. Certaines régions ont mis davantage l'accent sur la mise en œuvre de normes d'application volontaire et non contraignantes de comportement responsable des États par le truchement de mesures de renforcement des capacités, tandis que d'autres ont mis en place leurs propres mesures de confiance à l'échelon régional, en vue de réduire les risques de conflit découlant des activités liées aux TIC, ou ont adopté d'autres outils à l'échelon régional pour faire face aux menaces liées aux TIC. Divers instruments régionaux ont également été mis en place pour traiter certains aspects spécifiques des TIC.

Si les États assument la responsabilité première du maintien de la sécurité internationale, les TIC font partie intégrante de nos sociétés et la sécurisation du cyberespace revêt un intérêt particulier pour d'autres parties prenantes qui, dans ce domaine, jouent ont un rôle clé et assument des responsabilités.

De nombreuses et excellentes initiatives relatives au cyberespace ont été impulsées par le secteur privé. Il s'agit, par exemple, du Cybersecurity Tech Accord, dirigé par Microsoft, de la Charter of Trust, dirigée par Siemens et la Conférence de Munich sur la sécurité, et de la Global Transparency Initiative de Kaspersky Lab.

L'Appel de Paris pour la confiance et la sécurité dans le cyberespace de 2018, a réuni des entreprises, des États, des représentants de la société civile et des milieux universitaires, qui ont pris des engagements vis-à-vis de neuf principes relatifs à la cybersécurité. Ces principes couvrent un éventail de questions qui vont de l'élaboration de dispositifs destinés à empêcher la prolifération d'outils et de pratiques malveillants dans le domaine des TIC à la promotion de l'acceptation et de

[2] Voir le paragraphe 21 du rapport du Groupe d'experts gouvernementaux. Une version préliminaire du document est disponible à l'adresse suivante : https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

la mise en œuvre généralisées de normes internationales en matière de comportement responsable, en passant par des mesures de confiance concernant le cyberespace.

La conjugaison des perspectives du secteur privé, de la société civile et des milieux universitaires contribue de façon inédite et décisive à la mise au jour d'une solution collective au problème de la cybersécurité que recherche la communauté internationale.

L'ONU est quant à elle disposée à aider les États et les autres parties prenantes à promouvoir un environnement pacifique pour les TIC. À l'initiative du Secrétaire général, un Groupe de haut niveau sur la coopération numérique a mené des travaux puis déposé son rapport en 2019. Une série de tables rondes organisées par la suite avec des États et d'autres acteurs clés a permis d'élaborer un plan d'action dans lequel il a été recommandé de prendre de nouvelles mesures pour promouvoir la coopération dans des domaines clés de l'espace numérique.

En ce qui concerne la paix et la sécurité, le Secrétaire général a également lancé un programme de désarmement, qui met l'accent sur la compréhension et la gestion des technologies de nouvelle génération qui pourraient aller à l'encontre des normes juridiques, humanitaires et éthiques en vigueur, de la non-prolifération et de la paix et de la sécurité.

Dans le cadre de ce programme, le Secrétaire général s'engage à se concerter avec les scientifiques, les ingénieurs et les entreprises pour promouvoir l'innovation responsable dans les domaines des sciences et des technologies et garantir ainsi que ces dernières serviront à des fins pacifiques.

Il s'engage aussi à contribuer à promouvoir, de concert avec les États Membres, une culture de responsabilité et d'adhésion aux normes, règles et principes nouveaux relatifs à un comportement responsable dans le cyberespace.

Alors que presque tous les aspects de notre vie quotidienne reposent sur le cyberespace, l'ampleur et l'omniprésence des problèmes de l'insécurité liée aux TIC sont désormais considérées comme une menace majeure. La difficulté qu'il y a, sur les plans politique et technique, à identifier des responsables dans les cas d'attaques liées aux TIC pourrait avoir des conséquences considérables, y compris des réactions armées involontaires et une escalade.

Ces dynamiques peuvent pousser les États à adopter des postures offensives face à l'utilisation hostile de ces technologies. Elles peuvent également permettre à des groupes et à des individus criminels armés non étatiques de profiter d'un niveau élevé d'impunité pour mettre au point ou obtenir des capacités potentiellement déstabilisatrices. Compte tenu de ces incidences sur le maintien de la paix et de la sécurité internationales résultant des menaces liées aux TIC, l'apport du Conseil de sécurité dans ce domaine est primordial.

Je me félicite donc de cette occasion qui m'est donnée d'informer le Conseil, et j'attends avec le plus grand intérêt les délibérations à venir.

Annexe II

Déclaration de la Première Ministre de l'Estonie, M^me^ Kaja Kallas

L'Organisation des Nations Unies a été créée en prévision des temps à venir. Même si nous affrontons un certain nombre de difficultés nouvelles, les valeurs et les principes consacrés dans la Charte des Nations Unies il y a 76 ans restent toujours aussi valables aujourd'hui. La question de leur préservation dans un avenir de plus en plus numérique est devenue l'une des tâches les plus pressantes à l'échelle mondiale Aujourd'hui, je voudrais parler des perspectives et des menaces, ainsi que des mécanismes dont nous disposons pour faire face à cette situation.

Tout d'abord, au chapitre des perspectives : les dix-huit derniers mois que nous avons passés à travailler, à étudier et à vivre à distance ont clairement démontré que notre dépendance à l'égard des technologies numériques et des communications ne fera que croître avec le temps. Il nous incombe d'édifier un avenir où tous les acteurs respecteront certaines obligations dans leur comportement au sein du cyberespace.

C'est pourquoi le débat d'aujourd'hui ne porte pas sur la technologie mais sur la manière dont le cyberespace peut être utilisé. Steve Jobs l'a bien dit : « La technologie n'est rien. L'important, c'est de croire aux gens, de croire qu'ils sont fondamentalement bons et intelligents et que si vous leur donnez des outils, ils feront des merveilles ».

En tant que société numérique florissante, l'Estonie en a fait l'expérience directe. Un cyberespace libre, ouvert, stable et sûr fait partie de notre existence Nous économisons l'équivalent de 2 à 3 % de notre produit intérieur brut chaque année grâce à la mise en ligne de la plupart des services publics. Notre administration publique courante fonctionne sans papier depuis maintenant plus de 15 ans. L'Estonie a également produit le plus grand nombre de licornes technologiques par habitant.

Deuxièmement, les menaces : force est de reconnaître que le passage rapide au numérique comporte aussi des zones d'ombre.

Des acteurs malveillants peuvent utiliser le cyberespace pour causer des dégâts considérables. Imaginez, par exemple, ce qui se passerait si, au beau milieu d'une sécheresse, la chaîne d'approvisionnement en eau d'un pays cessait de fonctionner ou si, pendant le froid de l'hiver, le réseau électrique d'une nation subissait des perturbations.

Durant l'année écoulée, nous avons constaté à quel point des cyberattaques visant le secteur des soins de santé pouvaient constituer une menace réelle et tangible. Le fait de perturber des infrastructures critiques pourrait avoir des conséquences dévastatrices sur le plan humanitaire.

Les clôtures élevées et les gardes dont nous entourons nos centrales électriques et autres infrastructures critiques ne peuvent être d'un secours quelconque dans le cyberespace. Nous devons plutôt assumer collectivement le rôle de vigiles.

Enfin, comment faire face à ces menaces : heureusement, comme l'a souligné notre éminente conférencière, M^me^ Nakamitsu, nous disposons d'une base solide sur laquelle nous pouvons nous appuyer pour agir.

Au cours de la décennie écoulée, les États Membres sont convenus d'un cadre normatif effectif destiné à favoriser la stabilité du cyberespace et la prévention des conflits. Il s'agit du droit international en vigueur, de 11 normes d'application volontaire non contraignantes de comportement responsable des États et de mesures de confiance et de renforcement des capacités.

Le Danemark croit fermement que le droit international en vigueur, y compris la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international des droits de l'homme, s'applique dans le cyberespace.

Permettez-moi de souligner que les États sont responsables de tout acte commis en violation des obligations que leur impose le droit international.

De manière à assurer la protection des civils et des biens civils, notamment dans des situations de conflit armé – question dont débat régulièrement le Conseil de sécurité –, il est essentiel que toute utilisation des cybercapacités dans ce contexte soit soumise aux obligations découlant du droit international humanitaire.

Les 11 normes de comportement responsable des États dont nous sommes convenus reflètent les attentes de la communauté internationale et fixent d'importantes lignes directrices supplémentaires pour les activités des États dans le cyberespace.

Ce printemps, la communauté internationale a réaffirmé avec force l'importance de ce cadre normatif. Nous sommes encouragés et guidés par les conclusions encourageantes adoptées par consensus lors des dernières rencontres du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée. La mise en œuvre de ce cadre constitue un objectif majeur pour la communauté internationale.

Les actions engagées à l'échelle mondiale doivent être accompagnées, à l'échelon régional, par d'autres activités et par des mesures de renforcement des capacités. À cet égard, nous appelons l'attention sur l'importante action menée par les organisations régionales pour renforcer la confiance et promouvoir la coopération. L'Estonie accorde également la priorité aux initiatives qui visent à réduire la fracture numérique et qui doivent aller de pair avec le renforcement des capacités en matière de cyberrésilience et avec la protection des droits de de la personne en ligne.

Nous devons également prendre conscience de la nécessité d'aborder la question des cybermenaces en coopération avec le secteur privé, la société civile et les milieux universitaires. Les entreprises, en particulier, sont appelées à jouer un rôle important qui consiste à investir dans la cybersécurité et à contribuer à l'élimination des vulnérabilités.

Je suis convaincu que le débat de ce jour laissera une trace dans l'histoire du Conseil de sécurité, dans la mesure où nous abordons des questions qui revêtiront une importance certaine dans le maintien de la paix et de la stabilité internationales au cours des années à venir.

Notre avenir numérique ne sera assuré que si nous souscrivons à des règles communes.

Annex III

Déclaration du Premier Ministre du Niger, M. Mahamadou Ouhoumoudou

[Original : français]

Permettez-moi tout d'abord de saluer l'Estonie pour son engagement à placer la question des risques sécuritaires liés au cyberespace dans l'agenda du Conseil.

Je voudrais également remercier M^me^ Izumi Nakamitsu pour son intervention et son ferme engagement sur cette question.

Au cours des deux dernières décennies, la pénétration de l'Internet et l'utilisation des technologies de l'information et des communications (TIC) ont connu une croissance fulgurante. Le cyberespace est devenu de nos jours un enjeu de géopolitique permettant aux différentes nations d'avancer leur sphère d'influence tant au niveau économique, que politique et culturel.

Cette révolution numérique qui nous a tant rapproché en éliminant nos frontières, a aussi ouvert la voie à de nouveaux défis de souveraineté dus à la nature extraterritoriale de lois y attenantes. De la même manière que cet espace peut renforcer nos démocraties, en donnant une plateforme et un moyen à toutes les voix de se faire entendre, même les voix dissidentes, cet espace peut également s'avérer être un lieu de refuge pour des acteurs et groupes criminels dont le seul but est de déstabiliser nos nations.

La pandémie de la maladie à coronavirus (COVID-19) nous a montré les deux facettes de cet espace. D'un côté notre dépendance grandissante à l'égard des technologies numériques, cette réunion en format virtuel en est une preuve, et de l'autre, la fragilité de nos systèmes face aux possibilités de cybercriminalité et de cyberespionnage, démontré par les attaques criminelles employant des logiciels rançonneurs sur les systèmes de santé et les campagnes de désinformation ayant pour but de saper le moral des citoyens de nos pays contre les efforts de vaccination.

De plus, l'essor des réseaux sociaux et autres plateformes de discussions a donné lieu à la prolifération de certains types de discours incitant à des actes d'insurrection, de terrorisme, d'atteinte à nos valeurs morales et aux fondements de nos démocraties.

Eu égard à tout ce qui précède, permettez-moi de faire quelques recommandations susceptibles, de mon point de vue, de favoriser le renforcement du respect du droit international, ainsi que la mise en œuvre de règles d'engagement responsable des États dans le cyberespace.

Premièrement, il s'agit de la nécessité de combler la fracture numérique qui existe entre les nations, et principalement avec le continent africain, où les trois quarts des habitants n'ont pas un accès suffisant à Internet – ou n'y ont pas accès du tout.

Cette situation, comme l'ont mentionné les experts, est un facteur aggravant de la paupérisation des populations, et dont l'impact se répercute sur tout le monde et dans chaque composante de la société, de la santé au bien-être économique en passant par l'éducation et rend ces dernières davantage vulnérables aux campagnes de désinformation et autres menaces favorisées par le numérique. Nous ne pourrions espérer un cyberespace sain et protégé, sans pour autant s'assurer d'une équite numérique.

Sur cette base, ma deuxième recommandation est le développement d'une architecture mondiale à travers une approche intégrée et coordonnée, qui permettrait d'identifier, de manière claire, les règles de droit international applicables au cyberespace, dans des domaines aussi vastes que la santé, le droit international

humanitaire, les processus électoraux et les activités économiques, pour ne citer que ceux-là.

Mais ce faisant, nous devons également être conscients que cette architecture doit être équitable, tant au niveau de l'application que des avantages à exploiter, afin d'éviter de créer de nouveaux mécanismes à deux poids, deux mesures, qui ne feraient que creuser les inégalités entre les nations, en les obligeant à faire face à d'autres effets pervers.

Dans cette logique, il serait adéquat que toute nouvelle architecture réglementaire au plan mondial, s'inspire de celles déjà établies aux niveaux régionaux, qui sont censées harmoniser les réglementations applicables à l'échelle nationale des États. En ce sens, nous tenons à faire mention de la directive de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) sur la lutte contre la cybercriminalité, qui impose aux États membres des obligations en la matière, y compris la pénalisation de certains actes, et qui crée un cadre pour faciliter la coopération régionale en matière de cybersécurité.

Ma dernière recommandation serait que le Conseil de sécurité s'attèle à une interprétation plus inclusive et moins discriminatoire de la Charte des Nations Unies, mais aussi de son propre mandat, pour que nos délibérations puissent refléter la réalité du monde d'aujourd'hui, et pouvoir ainsi aborder les thématiques comme la cybersécurité, le changement climatique et les pandémies, car ces menaces sont réelles, et tout comme la COVID-19, ne connaissent pas de frontières.

Annexe IV

Déclaration du Ministre des affaires étrangères et de la défense de l'Irlande, M. Simon Coveney

Je voudrais adresser mes félicitations à l'Estonie pour sa présidence réussie du Conseil.

Je remercie la Haute Représentante pour les observations instructives dont elle nous a fait part.

Je me félicite de la tenue de ce débat fort opportun, qui est le premier du genre au Conseil de sécurité.

L'année dernière, le Secrétaire général a appelé les États à mettre de l'ordre dans ce qu'il a dénommé le « Far West du cyberespace ».

Si des progrès encourageants ont été enregistrés à l'échelon de l'Organisation des Nations Unies au cours de ces derniers mois, les difficultés auxquelles les États doivent faire face en matière de cybersécurité continuent de croître, mettant en danger la paix et la sécurité internationales.

Je voudrais axer mon intervention de ce jour sur trois points :

- Les difficultés et les perspectives ;
- La nécessité pour les États de mettre en œuvre les mesures convenues à l'ONU ;
- La nécessité de traiter cette question en s'appuyant sur des valeurs.

D'abord, les difficultés et les perspectives.

Les technologies numériques et des communications continuent de stimuler la croissance économique et de transformer notre façon de vivre, de communiquer et de travailler.

La gestion de certains grands problèmes mondiaux actuels, tels que le changement climatique, est largement tributaire de l'innovation. Celle-ci permet également d'enregistrer d'importantes avancées dans la recherche médicale, d'améliorer l'accès à l'éducation et de renforcer les capacités de nos soldats de la paix, contribuant ainsi à leur sécurité.

Durant l'année écoulée, la pandémie a mis en évidence notre dépendance croissante à l'égard des technologies de l'information et des communications, rapprochant les personnes à des moments où elles devaient se trouver éloignées les unes des autres, tout en faisant ressortir nos vulnérabilités.

S'agissant de ce dernier point, mes propos s'appuient sur une expérience récente. Le mois dernier, les systèmes de santé publique irlandais ont été victimes d'une attaque particulièrement dommageable, qui été perpétrée à l'aide de logiciels rançonneurs et a touché des services de santé essentiels.

La survenue d'une attaque de ce type durant une pandémie mondiale est consternante. Malheureusement, l'expérience irlandaise n'est pas isolée sur le plan international.

La cyberactivité malveillante, notamment les attaques paralysantes à l'aide de logiciels rançonneurs, la cybercriminalité, le vol de propriété intellectuelle et la diffusion de la désinformation et de la haine, a connu une forte augmentation ces dernières années.

Des infrastructures critiques sont de plus en plus visées.

L'Irlande est gravement préoccupée par le fait que cette activité constitue une menace pour la paix et la sécurité internationales.

Les problèmes de sécurité existants sont aggravés par des cybermenaces, telles que la vulnérabilité des systèmes de commande et de contrôle des armes nucléaires aux cyberattaques. Il devient d'autant plus urgent de progresser sur la voie du désarmement nucléaire.

Nous ne pouvons pas permettre que le cyberespace ne soit pas soumis à des règles ou à des lois et que des acteurs malveillants y opèrent à leur guise.

Les différends internationaux qui surviennent dans le cyberespace doivent être résolus par des moyens pacifiques.

Le Conseil doit se prononcer clairement en faveur d'un cyberespace mondial pacifique et sûr, fondé sur le consensus et la confiance mutuelle.

En ce qui concerne mon deuxième point, l'Irlande se félicite des avancées qui ont récemment été enregistrées l'ONU, en ce qui concerne l'adoption par consensus d'un cadre de comportement responsable des États dans le cyberespace.

Les États ont maintenant réaffirmé que le droit international en vigueur, en particulier la Charte des Nations Unies, constitue une base solide, fondée sur des règles, pour toutes les démarches qui sont entreprises dans le domaine de la cybersécurité.

L'Irlande soutient les initiatives qui visent à promouvoir une meilleure compréhension, par les États, de l'application du droit international au cyberespace.

Nous publierons bientôt notre position nationale et encourageons les autres à faire de même.

Le comportement responsable des États est, bien entendu, également primordial.

Tous les États Membres sont convenus de s'inspirer des 11 normes d'application volontaire de comportement des États dans le cyberespace.

Nous devons désormais nous attacher à promouvoir la compréhension et la mise en œuvre de ces normes, en nous appuyant sur les fondements du droit international, afin de renforcer la cybersécurité mondiale. Cette démarche permettra de réduire les risques de conflit et d'améliorer les relations internationales.

Les mesures de confiance, y compris le dialogue, permettent d'instaurer la confiance et de réduire les tensions entre les États. Je sais qu'il s'agit là d'une évidence, mais il faut que cela soit dit.

Nous nous félicitons du rôle de premier plan que jouent les organisations régionales à cet égard, notamment l'Organisation pour la sécurité et la coopération en Europe. L'Irlande et nos partenaires de l'Union européenne s'engagent à soutenir les initiatives relatives au renforcement des capacités.

Dans un cyberespace fortement interconnecté, aucun pays n'est en sécurité tant que tous les pays ne le sont pas. La pandémie de maladie à coronavirus (COVID-19) nous l'a bien enseigné.

Nous restons également déterminés à lutter contre la fracture numérique mondiale. L'accès en ligne pour tous sera un élément clé de la réalisation des objectifs de développement durable au cours de la prochaine décennie.

Mon troisième point est que le maintien de la paix et de la sécurité internationales dans le cyberespace doit être centré sur l'homme et fondé sur des valeurs.

L'Irlande est favorable à un cyberespace sûr, sécurisé et accessible, où les droits de la personne et les libertés fondamentales s'appliquent, tant en ligne que hors ligne.

Nous réaffirmons avec force l'applicabilité du droit international des droits de l'homme aux actions des États dans le cyberespace.

La protection des civils reste une priorité absolue dans tous les volets de nos activités. À ce sujet, l'Irlande est déterminée à assurer le respect du droit international humanitaire dans le cyberespace.

Il est regrettable que la violence fondée sur le genre subie par un trop grand nombre de femmes et de filles soit désormais souvent accompagnée et amplifiée par la violence en ligne et les cybermenaces.

Il est d'autant plus important, dans ces conditions, que les dirigeants que nous sommes – tous les dirigeants – nous attachions à promouvoir résolument la participation des femmes aux processus, décisions et politiques des Nations Unies relatives à la cybernétique.

Nous devons redoubler d'efforts pour combler le fossé numérique entre les sexes.

L'Irlande a toujours plaidé en faveur de la prise en compte d'un plus large éventail de compétences dans les débats de l'ONU relatifs à la cybersécurité et au renforcement des capacités.

Il incombe aux gouvernements et à ceux qui pilotent et dirigent l'innovation technologique de préserver la sécurité et la liberté dans le cyberespace.

Les contributions de la société civile, des experts techniques, des universitaires et du secteur privé ont enrichi les cyberdiscussions passées à l'ONU. À notre avis, leur participation au débat sur la cybersécurité a jusque-là été beaucoup trop limitée.

Nous soutenons également les initiatives, notamment l'Appel de Paris pour la confiance et la stabilité dans le cyberespace, qui rassemblent des acteurs étatiques et non étatiques dans le but commun de promouvoir la paix et la sécurité.

Nous devons tous œuvrer de concert pour trouver des solutions mieux partagées.

Pour conclure, l'Irlande continuera à soutenir les démarches constructives, multilatérales et multipartites, fondées sur le consensus, afin de renforcer la cyberrésilience dans le monde entier.

Nous appelons tous les États à se comporter de manière responsable, dans le plein respect du droit international, et à mettre en œuvre le cadre normatif.

Nous apprécions le rôle que joue le Conseil de sécurité dans la prévention des conflits et la promotion de la paix et de la sécurité, y compris dans le cyberespace.

Nous exhortons tous les États à mettre à profit les résultats obtenus à l'ONU au cours de ces derniers mois.

Nous pourrons ainsi garantir un cyberespace mondial plus sûr et plus pacifique, dont chacun pourra tirer parti.

Annexe V

Déclaration du Ministre des affaires étrangères du Viet Nam, M. Bui Thanh Son

Je remercie le Président du Conseil de sécurité d'avoir convoqué cette réunion sur un sujet particulièrement pertinent. Je remercie aussi la Secrétaire générale adjointe, M^me^ Nakamitsu, pour ses observations instructives.

Le développement fulgurant des technologies de l'information et des communications (TIC) a considérablement transformé la façon dont les gens vivent, travaillent et interagissent les uns avec les autres. Il a facilité la communication à l'échelle mondiale, le partage des connaissances et les échanges culturels, aidé les peuples et les pays à se rapprocher et également réorienté la production vers des modes plus efficaces, plus durables et plus inclusifs.

Cela étant, si elles tombent entre de mauvaises mains et sont utilisées de façon malveillante, ces technologies avancées peuvent constituer de graves menaces pour la souveraineté, la sécurité et la prospérité des nations. Utilisées par des terroristes ou par des criminels transnationaux, elles peuvent saborder des systèmes économiques, porter atteinte à la stabilité sociale et saper les valeurs culturelles et humanitaires.

Prenons le cas des pertes économiques causées par les cyberattaques. Les dépenses annuelles mondiales consacrées à la cybersécurité ont atteint 1 000 milliards de dollars en 2020, soit une augmentation de 50 % par rapport à 2018 et une multiplication par trois depuis 2013. Une bonne partie de ces dépenses est consacrée à la réparation des sinistres et à la reprise des activités.

Fait plus inquiétant encore, il a été fait état de cyberattaques transnationales qui avaient porté atteinte à la sécurité mondiale et nationale, en risquant même de déclencher une cyberguerre.

En tant que telle, la cybersécurité revêt un caractère urgent et primordial en ce qui concerne la paix, la sécurité, le développement et la prospérité, aux niveaux tant national que mondial. Dans ce contexte, je voudrais vous faire part des observations suivantes.

D'abord, chaque État dispose, dans le cyberespace, d'une souveraineté et d'intérêts propres qui doivent être pleinement respectés. C'est à chaque État Membre qu'incombe la responsabilité première de créer le cadre juridique qui régira, sur son territoire, le comportement de ses citoyens dans le cyberespace. Par ailleurs, la réglementation des comportements conformément à la loi, la prévention des actes malveillants illégaux et la facilitation des activités constructives sont des principes directeurs dont l'application permettra de créer un cyberespace sûr et stable au service de l'humanité et notamment de la paix et du développement.

Le Viet Nam est un pays à forte couverture Internet, où près de 70 % de la population utilisent effectivement l'Internet et les réseaux sociaux. Cette évolution tient à un cadre juridique global, qui facilite le développement des TIC et empêche leur utilisation abusive. Le Viet Nam accorde également la priorité à l'amélioration de l'autoprotection, de l'autonomie et de la résilience, associée à une coopération internationale effective.

Deuxièmement, les cyberattaques revêtent un caractère transnational, les réseaux Internet mondiaux devenant la cible d'une exploitation constante par les auteurs de ces attaques. Il faut donc trouver des solutions mondiales et transnationales aux problèmes liés à la cybersécurité. Le Viet Nam est favorable à la mise en place d'un cadre international qui détermine des règles et des normes de comportement responsable dans le cyberespace, sur la base d'un consensus et avec participation la

plus large possible des pays, et notamment aux processus en cours à l'ONU. Nous sommes préoccupés par l'utilisation malveillante et nocive des TIC, contre laquelle nous nous élevons, notamment les cyberattaques menées contre les installations essentielles que sont que les formations sanitaires, les systèmes électriques, les systèmes d'alimentation en eau et les installations alimentaires. Les activités entreprises dans le cyberespace doivent se conformer aux principes de la Charte des Nations Unies et du droit international, en particulier le respect de la souveraineté, la non-ingérence dans les affaires intérieures des États, le non-recours à la force et le règlement pacifique des différends.

Troisièmement, la consolidation de la coopération internationale, l'instauration de la confiance et l'application du principe de responsabilité sont indispensables au renforcement de la cybersécurité. Quels que soient leur taille et leur niveau de développement, tous les pays peuvent tirer parti d'un cyberespace mondial sécurisé et sûr. Ils doivent donc s'impliquer activement et participer de façon plus concrète et plus responsable en vue d'assurer la sûreté et la sécurité au sein du cyberespace mondial au profit de la paix, de la stabilité et du développement durable pour toutes les nations.

Le développement des TIC est une importante rampe de lancement dans notre quête commune de la prospérité. Le Viet Nam a activement mis en œuvre une stratégie nationale de transformation numérique. Nous voulons que l'économie numérique représente 30 % du produit intérieur brut d'ici à 2030. En Asie du Sud-Est, le Viet Nam a participé activement aux mécanismes régionaux de cybersécurité, notamment à la stratégie de coopération en matière de cybersécurité de l'Association des nations de l'Asie du Sud-Est. Nous entretenons également une coopération bilatérale effective avec de nombreux pays et partenaires internationaux dans ce domaine. Le Viet Nam est disposé à contribuer davantage au renforcement de la coopération internationale en faveur d'un cyberespace pacifique, stable, sécurisé et sûr au service de la prospérité et du développement durable de tous nos pays.

Annexe VI

Déclaration du Secrétaire du Gouvernement chargé des technologies de l'information et des communications, de l'innovation et de la jeunesse du Kenya, M. Joe Mucheru

Je félicite la Présidence d'avoir organisé, pour la première fois au Conseil de sécurité, un débat libre sur la cybersécurité. Je remercie la Haute-Représentante pour les affaires de désarmement, M^me^ Nakamitsu, pour son exposé instructif.

Notre dépendance croissante à l'égard des technologies de l'information et des communications (TIC) comporte à la fois des avantages et des inconvénients.

L'action de ceux qui mettent au point et utilisent les TIC et les technologies émergentes à des fins pacifiques est pratiquement égalée par celle des parties adverses qui utilisent ces technologies à des fins de mainmise, de surveillance illicite, de fraude, de radicalisation et de déstabilisation.

Le Kenya milite en faveur de la préservation et de la protection d'un domaine Internet libre et ouvert. Il s'agit pour nous d'un moteur essentiel du développement national et nous nous employons à ce que nos jeunes acquièrent les compétences et le niveau de compétitivité voulues dans son utilisation.

Nous sommes un leader mondial dans le domaine de la monnaie numérique, ayant été le pionnier de M-Pesa, la première plateforme d'argent mobile largement utilisée. Notre Gouvernement a également institué une plateforme numérisée de services publics dispensés par l'intermédiaire de terminaux de services faisant office de guichets uniques, connus sous le nom de centres Huduma et disséminés dans tout le pays.

Les jeunes Kenyans innovent et créent des entreprises transformatrices. Les investisseurs du monde entier en ont donné acte, notre « Silicon Savanna » attirant le plus d'investissements dans notre région. Nous sommes convaincus qu'à l'avenir bon nombre de nos emplois décents seront liés à ces entreprises.

En raison de cette large ouverture sur le secteur numérique, la sécurisation des TIC constitue, pour le Kenya, un objectif prioritaire du secteur de la sécurité nationale.

Dans cette optique, nous nous sommes dotés d'un important régime de réglementation. Face aux menaces, nos capacités de réaction vont croissant. Notre équipe d'intervention informatique d'urgence collabore avec d'autres équipes nationales d'intervention informatique d'urgence et, sur le plan international, avec le « global Forum of Incident Response and Security Teams » (« Forum mondial des équipes d'intervention en cas d'incidents liés à la sécurité informatique »).

Notre tâche aujourd'hui consiste à formuler des propositions sur la manière dont le Conseil de sécurité pourrait mieux assurer la paix et la sécurité internationales face aux menaces que véhicule ou rend possibles le cyberespace.

Je voudrais dégager trois domaines qui, selon nous, tireraient parti d'un renforcement de la coopération et de la collaboration internationales.

Le premier domaine concerne les TIC et les économies émergentes. La cybercriminalité se focalise de plus en plus sur les économies émergentes. Il faut coopérer davantage pour renforcer les mécanismes régionaux et internationaux existants de règlement des conflits économiques, et notamment coordonner les initiatives qui visent à identifier et à atténuer les risques que posent les activités liées

aux TIC, comme la fraude numérique, l'impact des crypto-monnaies sur les banques centrales nationales et les cyberattaques contre les infrastructures critiques.

À mesure que l'automatisation industrielle s'accélère, il convient de remplacer les emplois perdus par d'autres emplois décents, sous peine de compromettre la paix et la sécurité. Il faudra s'employer davantage à investir dans les compétences numériques qui permettent aux pays dont l'industrie est sous-développée d'attirer des investissements susceptibles de créer des millions de nouveaux emplois.

Le deuxième domaine concerne les TIC et l'extrémisme violent. Parce qu'elles sont omniprésentes, programmables et guidées par les données, les technologies émergentes, tout en comportant des avantages, se prêtent également à une utilisation abusive par les groupes armés et les terroristes. Ces groupes mettent à profit l'opacité des mécanismes de contrôle, les algorithmes, l'impression 3D, la cryptographie et l'interface utilisateur simplifiée pour effectuer des recrutements et pour planifier et réaliser des actes de terrorisme. La radicalisation et la militarisation s'en sont trouvées renforcées.

Le Kenya appelle à un renforcement de la coopération entre le Conseil de sécurité et le Bureau de lutte contre le terrorisme, qui permette d'instituer un dispositif efficient de sécurisation du cyberespace, capable de répondre aux besoins des États Membres dans le domaine du renforcement des capacités.

Les mandats des opérations de paix des Nations Unies devront également prendre en compte l'utilisation du cyberespace par des acteurs militarisés hostiles.

Mon troisième domaine d'intérêt est celui des TIC et des médias sociaux. On ne saurait trop souligner l'impact croissant des infox, des hypertrucages et des informations fausses et trompeuses sur la paix et la sécurité. Nous avons récemment pu constater l'impact des infox qui ont battu en brèche les interventions menées face à la pandémie de maladie à coronavirus (COVID-19), en encourageant les hésitations face à la vaccination.

Les entreprises de médias sociaux devront avoir à répondre de leurs actes et être amenées à s'assurer que les infox, en particulier celles émanant d'acteurs sophistiqués, dont certains sont soutenus par des États, ne prolifèrent pas sur leurs plateformes. Il faudra fonder cette réglementation sur une plateforme multilatérale pour garantir l'uniformité de ses effets.

Je conclus en affirmant que le Kenya est disposé à contribuer au renforcement des initiatives mondiales, des cadres institutionnels et des normes qui rendront davantage possible la mise en place d'un cyberdomaine libre, pacifique et stable, tout en atténuant les menaces.

Annexe VII

Déclaration de la Représentante permanente des États-Unis d'Amérique auprès de l'Organisation des Nations Unies, M^me^ Linda Thomas-Greenfield

Je remercie la Présidence et l'Estonie d'avoir organisé l'important débat de ce jour. Nous sommes profondément reconnaissants à l'Estonie d'avoir porté cette question à l'attention du Conseil. Je remercie par ailleurs la Haute-Représentante, M^me^ Nakamitsu, pour son exposé instructif.

Le présent débat intervient à un moment opportun. Du fait de la survenue de la pandémie de maladie à coronavirus (COVID-19) en particulier, nous n'avons jamais autant compté sur la technologie, et nous le constatons aujourd'hui. Mais tant les acteurs étatiques que les acteurs non étatiques mettent à profit ce surcroît de dépendance. Aux États-Unis, différents logiciels rançonneurs très médiatisés ont perturbé le fonctionnement de JBS, une grande entreprise agro-alimentaire, et de la Colonial Pipeline, une entreprise qui assure l'alimentation en carburant d'une grande partie de la côte est. Ces évènements témoignent de la gravité et du caractère inacceptable du risque que la cybercriminalité fait peser sur les infrastructures critiques. Très souvent, les effets de ces activités malveillantes ne se cantonnent pas non plus à l'intérieur des frontières. Par exemple, la cyberactivité malveillante a ciblé l'entreprise de logiciels SolarWinds et le logiciel Exchange Server de Microsoft.

Le risque est évident. Notre infrastructure – en ligne et hors ligne – est en jeu. Nos services les plus essentiels et les plus critiques – des aliments que nous mangeons à l'eau que nous buvons, en passant par les services de soins de santé sur lesquels nous avons tous compté pendant la pandémie – sont des cibles. Par conséquent, dans le monde actuel, lorsque nous parlons de sécurité globale, nous devons également parler de cybersécurité. Fort heureusement, malgré nos différences idéologiques, les États Membres se sont retrouvés à plusieurs reprises au cours de la dernière décennie pour tenter de prévenir les conflits que pourraient engendrer les cybercapacités. Ensemble, nous avons défini un cadre de comportement responsable des États dans le cyberespace, par le truchement du Groupe d'experts gouvernementaux. Il est clairement précisé, dans ce cadre, que le droit international s'applique au cyberespace. Il y est également défini des normes d'application volontaire et les mesures de coopération pratiques que les États devraient prendre.

Au cours de ces derniers mois, le Groupe de travail à composition non limitée, composé de tous les États Membres, est parvenu à un consensus sur un nouveau rapport qui entérine explicitement le cadre de comportement responsable des États dans le cyberespace. Le mois dernier, la sixième réunion du Groupe d'experts gouvernementaux des Nations Unies a abouti à l'adoption d'une série de recommandations consistantes et d'orientations nouvelles concernant le cadre. Il s'agit là d'une avancée. Ces rapports fournissent des orientations concrètes sur diverses questions, qui vont de l'utilisation des cybercapacités par les États à l'approche de la question complexe de l'attribution des cyberincidents. Le cadre traite également de la manière dont les États devraient coopérer pour atténuer les effets d'une cyberactivité malveillante grave émanant du territoire d'un État donné, y compris les activités menées par des criminels.

Nous partageons tous cette responsabilité. Comme l'a récemment déclaré le président Biden, et je cite, « les pays doivent prendre des mesures contre les criminels qui utilisent des logiciels rançonneurs sur leur territoire ». Soyons donc clairs : lorsqu'un État est informé d'une activité préjudiciable émanant de son territoire, il

doit prendre des mesures raisonnables pour y remédier. Compte tenu du caractère transnational du cyberespace, cette coopération est essentielle.

Le cadre que les États membres se sont donné tant de mal à élaborer constitue désormais le code de la route. Nous nous sommes tous engagés vis-à-vis de ce cadre. Il est désormais temps de le mettre en œuvre. Il nous reste encore beaucoup à faire pour garantir que tous les États qui veulent agir de manière responsable dans le cyberespace disposent à la fois des connaissances et des capacités techniques nécessaires. Parallèlement au travail que nous réalisons, nous devons continuer à protéger la liberté de l'Internet. Les droits dont jouissent les personnes hors ligne – notamment les droits à la liberté d'expression, d'association et de réunion pacifique – doivent également être protégés en ligne.

Les États membres ont fait montre d'une volonté remarquable, s'agissant de surmonter les différences et de parvenir à un consensus sur ces questions. Continuons à manifester cette bonne foi et offrons au monde un front uni dans le domaine de la cybersécurité. Ensemble, nous pourrons mettre sur pied un cyberespace ouvert, sécurisé et stable dont tout un chacun tirera parti.

Annexe VIII

Déclaration du Ministre des affaires étrangères de l'Inde, M. Harsh Vardhan Shringla

Je remercie la Présidence et salue l'initiative qu'a eue l'Estonie d'organiser ce débat public pour mettre en lumière l'important domaine émergent qu'est la cybersécurité. Je remercie la Secrétaire générale adjointe, M^me^ Nakamitsu, pour son exposé.

Si le concept de la paix est resté constant depuis la création du Conseil de sécurité, la nature des conflits et les éléments qui les sous-tendent ont considérablement évolué au fil des décennies. Aujourd'hui, nous sommes témoins de menaces qui, provenant du cyberespace, pèsent de plus en plus sur la sécurité des États Membres et ne peuvent plus être ignorées. Ce débat public est donc opportun.

L'utilisation croissante des cybertechnologies et des technologies de l'information et des communications (TIC) a accéléré le développement économique, amélioré la prestation des services aux citoyens, renforcé la conscience sociale et mis l'information et la connaissance à la disposition de tout un chacun. Qu'elles soient politiques, sociales, économiques, humanitaires ou liées au développement (y compris la présente réunion de haut niveau du Conseil de sécurité), la plupart des activités de cette ère cybernétique sont désormais menées dans le cyberespace ou associées à celui-ci. La pandémie de maladie à coronavirus (COVID-19) n'a fait qu'accélérer et étendre la numérisation de ces activités.

La dynamique et le caractère évolutif du cyberespace ont également introduit la cybersécurité dans le discours sur la paix et la sécurité. Le caractère transfrontalier du cyberespace et, plus important encore, l'anonymat des acteurs impliqués ont remis en question les concepts traditionnellement acceptés de souveraineté, de juridiction et de vie privée. Ces caractéristiques particulières du cyberespace posent de nombreux problèmes aux États Membres. Je me focaliserai sur trois problèmes clés :

Premièrement, certains États se servent des compétences dont ils disposent dans le domaine du cyberespace pour poursuivre des objectifs politiques et sécuritaires et pour se livrer à des formes modernes de terrorisme transfrontalier. Le monde constate déjà comment il est fait appel à des cyber-outils pour compromettre la sécurité des États, notamment en attaquant des infrastructures nationales critiques, telles que des installations sanitaires et énergétiques, et même en perturbant l'harmonie sociale par la radicalisation. Les sociétés ouvertes se sont révélées particulièrement vulnérables aux cyberattaques et aux campagnes de désinformation.

Deuxièmement, nous voyons les terroristes du monde entier utiliser avec sophistication le cyberespace pour élargir leur audience, diffuser une propagande virulente, inciter à la haine et à la violence, recruter des jeunes et recueillir des fonds. Les terroristes ont également utilisé les médias sociaux pour planifier et exécuter leurs attaques terroristes et causer des préjudices considérables. En tant que victime du terrorisme, l'Inde a toujours souligné la nécessité pour les États Membres d'aborder et de traiter de manière plus stratégique les implications de l'exploitation terroriste du cyberdomaine.

Troisièmement, l'intégrité et la sécurité des produits des TIC, qui sont des pièces maîtresses du cyberespace, sont compromises. Nombreux sont celles et ceux qui s'inquiètent du fait que des acteurs étatiques et non étatiques introduisent, notamment par le truchement de portes dérobées, des vulnérabilités et des fonctions cachées malveillantes dans les réseaux et les produits des TIC. Ces actes malveillants sapent la confiance à l'égard de la chaîne d'approvisionnement mondiale des TIC, compromettent la sécurité et pourraient devenir des points chauds entre les États. Il

est de l'intérêt de la communauté internationale de veiller à ce que tous les acteurs respectent leurs obligations et leurs engagements internationaux et ne se livrent pas à des pratiques qui pourraient désorganiser les chaînes d'approvisionnement mondiales et le commerce des produits des TIC.

Du fait de l'interconnexion du cyberdomaine, il n'est pas possible de mettre au jour, de manière isolée, des solutions aux problèmes et aux menaces complexes qui émanent du cyberespace. Dans le domaine du cyberespace, les États Membres que nous sommes devons adopter une stratégie de collaboration fondée sur des règles et œuvrer en vue de garantir l'ouverture, la stabilité et la sécurité de ce secteur. La dynamique créée par les résultats engageants des travaux du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et du Groupe de travail à composition non limitée sur l'évolution des TIC devrait être mise à profit pour trouver un nouveau terrain d'entente et améliorer les normes et les règles déjà convenues concernant le cyberespace. Ces règles doivent permettre de garantir une cybersécurité collective grâce à la coopération internationale. Une participation multipartite jouera un rôle déterminant dans la réalisation de cet objectif.

La promotion d'un accès équitable au cyberespace et à ses avantages devrait constituer un autre élément important de cette coopération internationale. L'élargissement du « fossé numérique » et de « l'écart des compétences numériques » entre les pays crée un environnement non viable dans le domaine du cyberespace. La dépendance croissante au numérique depuis le déclenchement de la maladie à coronavirus 2019 (COVID-19) a exacerbé les risques et mis en lumière ces inégalités face au numérique. Ces problèmes doivent être résolus par le renforcement des capacités. Il ressort du caractère omniprésent et transfrontalier du cyberespace que nous ne sommes pas plus forts que le maillon le plus faible du réseau mondial. « Ensemble seulement » nous pourrons atteindre l'objectif d'un cyberespace résilient et sécurisé au niveau mondial et nous devons veiller à ce qu'aucun pays ne soit laissé de côté dans cette entreprise collective.

L'Inde souscrit à un cyberespace ouvert, sûr, libre, accessible et stable, qui deviendra un moteur pour l'innovation, la croissance économique et le développement durable, garantira la libre circulation de l'information et respectera la diversité culturelle et linguistique. Grâce aux initiatives que nous avons lancées ces dernières années dans le domaine des technologies transformatrices, comme IndiaStack, Aadhar et UPI, nous avons réussi à tirer parti de l'énorme potentiel des cybertechnologies pour mettre en œuvre le Programme de développement durable à l'horizon 2030 et pour améliorer la gouvernance. Dans le cadre de sa campagne de vaccination contre la COVID-19, l'une des plus importantes au monde, l'Inde a mis au point Co-WIN, une plateforme technologique modulable, inclusive et ouverte. La plateforme Co-WIN peut être adaptée et transposée à une plus grande échelle pour des interventions en santé dans le monde entier. Nous nous employons à partager cette plateforme avec les pays partenaires.

Notre objectif premier est de mettre le cyberespace au service de la croissance et de l'autonomisation, non seulement dans notre pays, mais pour l'humanité tout entière. L'Inde est disposée à offrir ses compétences et à partager son expérience dans cette entreprise.

Annexe IX

Déclaration de la Ministre d'État chargée des affaires étrangères et du commerce extérieur de Saint-Vincent-et-les-Grenadines, M^me^ Keisal M. Peters

Nous tenons à remercier la présidence estonienne d'avoir pris l'initiative d'organiser le débat public de haut niveau de ce jour sur un sujet d'une importance capitale, afin de faire le point sur l'action que mène le Conseil de sécurité dans le cadre de sa mission de maintien de la paix et de la sécurité internationales. Je voudrais également remercier tous les intervenants de ce jour pour leurs exposés instructifs.

Dans le monde d'aujourd'hui, le cyberespace affecte presque tous les aspects de notre vie quotidienne. Le rôle que jouent les technologies de l'information et des communications (TIC) dans la réalisation de gains économiques et sociaux est évident. Toutefois, en dépit de ces atouts, le monde doit rester conscient des graves problèmes que posent les TIC. L'environnement mondial des TIC doit faire face à un développement spectaculaire de l'utilisation malveillante des TIC par des acteurs étatiques et non étatiques. De fait, l'utilisation abusive des TIC fait peser des risques pour tous les États et peut avoir des répercussions préjudiciables sur la paix et la sécurité internationales. Nous devons donc impérativement nous appuyer sur un engagement antérieur pour instituer des mesures de confiance qui renforcent la paix et la sécurité internationales et améliorent la coopération, la transparence, la prévisibilité et la stabilité entre les États Membres dans ce domaine.

Un environnement ouvert, sûr, stable, accessible et pacifique en matière de TIC est essentiel pour tout un chacun et exige une coopération effective entre les États, qui permette de réduire les risques pour la paix et la sécurité internationales. En outre, d'autres acteurs dotés de capacités et d'aptitudes différentes, issus de différents secteurs et à tous les niveaux de la chaîne mondiale des TIC, jouent un rôle essentiel dans la sauvegarde de la cybersécurité. Nous devons étudier les possibilités de mobilisation de ressources supplémentaires en vue du renforcement des capacités et de la mise à disposition de l'assistance technique. L'Organisation des Nations Unies doit renforcer l'assistance aux États Membres et contribuer à assurer la cohérence des actions que mènent ses différentes entités qui interviennent dans le cyberespace. Ces interventions doivent s'inscrire dans les objectifs d'ensemble de l'Organisation.

Malgré les nombreuses difficultés auxquelles nous devons faire face en tant que petit État insulaire en développement, Saint-Vincent-et-les-Grenadines a pris des mesures concrètes pour améliorer sa capacité à lutter contre le fléau de la cybercriminalité. Deux lois – la Loi sur la preuve électronique (Electronic Evidence Act) de 2004 et la Loir sur les transactions électroniques (Electronic Transactions Act) de 2007 – constituent le cadre législatif de base de la cybersécurité dans le pays. En août 2016, les législateurs ont adopté le projet de loi sur la cybercriminalité de 2016, dotant ainsi le pays d'un droit substantiel et procédural censé lui permettre de lutter de manière plus effective contre la cybercriminalité. Nous sommes également déterminés à honorer les accords régionaux auxquels nous avons souscrit en matière de cybersécurité au sein de l'Organisation des États américains (OEA) et de la Communauté des Caraïbes (CARICOM).

En raison de la pandémie de maladie à coronavirus (COVID-19) et d'autres perturbations causées par la récente éruption volcanique, les écoles de notre pays sont passées à l'enseignement à distance, comme c'est le cas partout dans le monde. Le Gouvernement ayant remis des tablettes à des milliers d'enfants pour faciliter cette transition, l'utilisation de l'Internet et le temps passé devant les écrans ont augmenté. C'est pourquoi le Ministère de l'éducation et de la réconciliation nationale a lancé la

campagne #GoCyberSmart en vue de promouvoir la cybersécurité. La campagne est une initiative de sensibilisation destinée à permettre aux étudiants de prendre les bonnes décisions en matière numérique. Les trois domaines d'intervention sont la sécurité de l'information, la sécurité du matériel et la sécurité de la navigation en ligne.

Les échanges d'informations à l'échelon des États Membres et des organisations régionales et internationales jouent un rôle essentiel qui consiste à garantir la stabilité et à prévenir l'escalade des cyberincidents. Nous appelons, d'autre part, les États Membres à continuer de respecter le droit international et le cadre de comportement responsable des États dans le cyberespace.

Dans l'action que nous menons pour promouvoir le comportement responsable des États dans le cyberespace, dans le contexte de la paix et de la sécurité internationales, nous devons nous inspirer des évaluations et des recommandations figurant dans les rapports de consensus du Groupe d'experts gouvernementaux de 2010, 2013, 2015 et, plus récemment, de 2021, ainsi que des conclusions et des recommandations du rapport final du Groupe de travail à composition non limitée des Nations Unies.

En conclusion, l'absence d'accords sur les règles d'engagement, les normes politiques et les mécanismes de coopération internationale pour un environnement pacifique des TIC ne ferait que créer de nouvelles sources d'instabilité et de conflit. Dans le cyberespace, nous encourageons tous les acteurs de la communauté internationale à honorer leurs obligations juridiques internationales, y compris le respect de la souveraineté et de l'indépendance politique, consacré dans la Charte des Nations Unies, et les principes de règlement pacifique des différends, de la même manière que dans le monde physique. La dynamique enclenchée en faveur du maintien de la paix et de la sécurité internationales dans le cyberespace ne doit jamais s'estomper.

Annexe X

Déclaration du Vice-Ministre des affaires étrangères de la Norvège, M. Audun Halvorsen

Un cyberespace mondialement accessible, libre, ouvert et sécurisé est essentiel au maintien de la paix et de la sécurité internationales. Nous nous félicitons que l'Estonie ait porté cette question à l'attention du Conseil de sécurité – le principal organe de l'ONU responsable du maintien de la paix et de la sécurité internationales, conformément à la Charte des Nations Unies.

Les technologies de l'information et des communications (TIC) sont un élément fondamental de l'infrastructure mondiale. Elles sont au cœur du développement, de la stabilité et de la sécurité de tous les États. Pourtant, le cyberespace devient aussi de plus en plus une arène de compétition et de conflit potentiel entre les États.

Au cours de la dernière décennie, nous avons vu comment les cyberopérations malveillantes, menées par des États et des acteurs non étatiques, ont gagné en portée, en ampleur, en gravité et en sophistication. Nous nous trouvons au beau milieu d'une pandémie mondiale, au moment où même des infrastructures sanitaires critiques ont été la cible de ces activités malveillantes, mettant en danger la sécurité des personnes et compromettant les actions que nous menons à l'échelle mondiale pour gérer la crise de la COVID-19.

Il existe aussi, cependant, des raisons d'être optimiste. L'année dernière, la démonstration a été faite que la communauté internationale était disposée à se montrer à la hauteur de la situation et à coopérer pour promouvoir un comportement responsable des États dans le cyberespace. Les rapports de consensus du Groupe de travail à composition non limitée et du Groupe d'experts gouvernementaux témoignent de l'engagement de tous les États Membres à veiller au respect de l'ordre international fondé sur des règles dans le cyberespace. C'est une victoire pour le multilatéralisme.

L'affirmation de l'applicabilité du droit international au cyberespace est la pierre angulaire des rapports de consensus du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée. Le droit international est le fondement de l'engagement commun des États à prévenir les conflits et à maintenir la paix et la sécurité internationales. Il joue un rôle essentiel dans le renforcement de la confiance entre les États. Les auteurs des deux rapports réaffirment que le droit international, et 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 ouvert, sûr, stable, accessible et pacifique pour les TIC.

Nous considérons comme une avancée majeure le fait que le Groupe d'experts gouvernementaux ait reconnu, dans son rapport, que le droit international humanitaire s'applique à tous les conflits armés, y compris dans le contexte du cyberespace.

Le droit international humanitaire vise à réduire au minimum les souffrances humaines causées par les conflits armés. Il réglemente et limite les cyberopérations pendant les conflits armés, tout comme il réglemente et limite tout autre moyen et méthode de combat. Par conséquent, les attaques contre les civils ou les biens civils sont interdites et les services médicaux doivent être protégés et respectés. Il est donc interdit d'attaquer les infrastructures critiques, telles que celles ayant trait à l'approvisionnement en électricité, à la production alimentaire, aux installations d'eau potable ou à autres objets indispensables à la survie de la population.

Reconnaître l'applicabilité du droit international humanitaire dans le cyberespace ne légitime pas la cyberguerre. Tout recours à la force par les États reste

régi par la Charte des Nations Unies et les règles pertinentes du droit international coutumier. Les différends internationaux doivent être réglés par des moyens pacifiques, dans le cyberespace comme dans tous les autres domaines.

Tous les États Membres se sont prononcés en faveur d'un cadre de comportement responsable des États dans le cyberespace, qui est fondé sur l'applicabilité du droit international, l'adhésion à des normes d'application volontaire convenues, des mesures de confiance concrètes et des mesures de renforcement des capacités, l'objectif visé consistant à consolider la résilience et la sécurité de tous. Il s'agit d'une avancée considérable, qui ne peut toutefois se concrétiser que si ce cadre est mis en œuvre et respecté par tous les États.

La réunion de ce jour consiste en une reconnaissance du fait que les activités malveillantes menées dans le cyberespace peuvent avoir de graves répercussions sur la paix et la sécurité internationales. Il s'agit également d'un message clair adressé à tous les États : il est attendu de nous que nous soyons à la hauteur du cadre de comportement responsable des États dans le cyberespace, dont nous sommes convenus nous devons honorer les obligations que nous impose le droit international et adhérer aux normes auxquelles nous avons souscrit.

Annexe XI

Déclaration du Ministre d'État chargé de l'Asie du Sud et du Commonwealth du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Lord Ahmad of Wimbledon

Aujourd'hui, presque tout a une dimension numérique.

La communauté internationale doit saisir les possibilités remarquables qu'offre l'Internet pour l'apprentissage, les affaires, la communication et, bien sûr, les loisirs.

Mais nous devons également traiter les menaces connexes avec le sérieux qui convient.

Les menaces que posent les activités malveillantes et dangereuses dans le cyberespace sont aujourd'hui plus évidentes que jamais.

En effet, le mois dernier seulement, une bande criminelle a pris pour cible Colonial Pipeline, exigeant une rançon du plus grand pipeline de carburant d'Amérique et menaçant de graves perturbations économiques.

Une partie de cette activité vise le vol ou l'extorsion. Souvent, il s'agit simplement d'actes de sabotage et de perturbations.

Mais, en tant que communauté internationale, nous assumons une responsabilité collective qui consiste à mettre en place un cyberespace qui profite à tous les pays et, de fait, à tout un chacun. Ensemble, nous devons façonner les règles qui serviront le bien commun.

Bien entendu, nous ne partons pas de zéro dans ce domaine.

Il y a dix ans, le Royaume-Uni a réuni plus de 60 pays à Londres pour établir des principes de base tels que l'accès universel à l'Internet et la protection des droits des personnes en ligne.

Dix ans plus tard, nous avons parcouru un long chemin.

Cette année seulement, l'Assemblée générale a réaffirmé à l'unanimité l'application du droit international dans le cyberespace et a adopté un ensemble de principes d'application volontaire, portant par exemple sur la nécessité d'assurer la protection des infrastructures de santé.

Un groupe d'experts gouvernementaux a enrichi notre compréhension des normes, règles et principes du cyberespace et a formulé des interprétations claires de l'application du droit international.

Mais nous devons aller encore plus loin. Ce n'est un secret pour personne que des États mènent des cyberopérations à l'appui de leurs capacités militaires et de sécurité nationale. Le Royaume-Uni en fait partie.

Que les choses soient bien claires : nous utiliserons ces capacités pour nous défendre contre ceux qui cherchent à nous nuire. Nous nous engageons à utiliser ces capacités en cas de besoin, de manière proportionnée et dans le respect du droit international.

Notre défi collectif consiste à préciser la manière dont les règles du droit international s'appliquent aux activités des États dans le cyberespace, à nous prémunir contre les acteurs malveillants qui contournent les règles et à faire en sorte que ceux qui se livrent à une cyberactivité malveillante en paient le prix.

Le Royaume-Uni est résolu à œuvrer de concert avec tous les pays et avec ses nombreuses parties prenantes, afin de garantir que le cyberespace est régi par des

règles et des normes qui renforcent notre sécurité collective, contribuent à la promotion des valeurs démocratiques, soutiennent la croissance économique mondiale et font obstacle à la propagation de l'autoritarisme numérique.

Nous devons faire respecter l'État de droit dans le cyberespace en incarnant le comportement responsable des États, en encourageant le respect des règles, en décourageant les attaques et, bien entendu, en exigeant des autres qu'ils rendent des comptes en cas de comportement irresponsable d'un État.

Nous devons également accorder une priorité absolue à la protection des droits de l'homme en ligne, comme hors ligne, de manière à instituer un cyberespace libre, ouvert, pacifique et sûr, accessible à tous.

Le cadre des Nations Unies pour un comportement responsable des États dans le cyberespace est notre point de départ. Nous devons aider tous les États à l'appliquer désormais.

Le Royaume-Uni a annoncé, le mois dernier, qu'il investirait plus de 30 millions de dollars pour soutenir le renforcement des capacités en matière de cybernétique dans les pays vulnérables, en particulier en Afrique et dans la région indo-pacifique.

L'action que nous menons avec Interpol aidera les pays, dont l'Éthiopie, le Ghana, le Nigéria, le Rwanda et le Kenya, à appuyer des opérations conjointes contre les cybercriminels.

Ailleurs, le financement britannique contribuera à la mise en place d'équipes nationales d'intervention d'urgence, qui assureront la protection des pays contre ces menaces.

Nous ne pourrions évidemment rien faire sans nos partenaires du secteur privé et, bien entendu, des milieux universitaires et de la société civile.

Mais, cela étant, nous sommes réunis ici aujourd'hui car le Conseil de sécurité a également un rôle central et important à jouer.

Lorsque des activités malveillantes comportent des risques pour la paix et la sécurité internationales, en exacerbant un conflit ou en provoquant des crises humanitaires, le Conseil de sécurité doit être disposé à intervenir.

Le Conseil doit réagir comme il le ferait face à des menaces posées par des moyens conventionnels.

Nous pouvons saisir les possibilités qu'offre le cyberespace et faire en sorte qu'il demeure, pour tous, un moteur pour la prospérité et le progrès.

Pour ce faire, il est essentiel que nous coopérions pour contrer ceux qui veulent mettre en danger notre sécurité collective.

Je voudrais enfin vous assurer de ceci : le Royaume-Uni est pleinement déterminé à protéger un cyberespace libre, ouvert, pacifique et sécurisé pour les générations à venir.

Annexe XII

Déclaration du Ministre délégué auprès du Ministre de l'Europe et des affaires étrangères de la France, M. Franck Riester

[Original : français]

Je tiens à remercier la Première Ministre d'Estonie pour cet évènement. Le Conseil de sécurité veille au maintien de la paix et de la sécurité internationales et doit pouvoir le faire dans le cyberespace.

Le cyberespace est un lieu d'opportunités mais également de nouvelles menaces. Il est devenu un terrain de compétition stratégique entre puissances. Les usages malveillants des technologies de l'information et des communications (TIC), par des acteurs étatiques comme non étatiques, prolifèrent.

Nous l'avons constaté au cours de ces dernier mois, notamment dans le contexte de la pandémie de maladie à coronavirus (COVID-19) qui a accentué notre dépendance à ces technologies. Je pense d'abord aux cyberattaques odieuses par logiciels rançonneurs menées contre des hôpitaux et d'autres infrastructures critiques. Je veux exprimer toute la solidarité de la France avec les victimes de ces attaques. Je pense également aux campagnes de manipulations de l'information au travers de la propagation des « infodémies » ou encore à la fragmentation croissante de l'Internet, des pratiques qui sont contraires aux valeurs démocratiques. Les actions dans le cyberespace ont des conséquences bien réelles et peuvent s'avérer brutales, dans nos vies et nos sociétés.

L'enjeu pour le siècle à venir sera de bâtir une gouvernance et une régulation collective du cyberespace. Nous ne voulons pas d'un « Far West » numérique, ni d'un cloisonnement du cyberespace. Nous l'avons affirmé dans l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, ainsi que dans le cadre du Groupe des Sept (G7) par la Déclaration de Dinard sur l'initiative pour les normes dans le cyberespace. La France est déterminée à bâtir avec ses partenaires un cyberespace ouvert, sûr, stable, non fragmenté, accessible et pacifique.

Le droit international, y compris la Charte des Nations Unies, s'applique dans son intégralité au cyberspace. Cela implique aussi le respect du droit international humanitaire par les opérations cyber conduites lors des conflits armés.

Face à la multiplication des menaces dans le cyberespace et des cyberattaques, les gouvernements doivent répondre par la coopération et le droit. Depuis plus d'une décennie, la France a joué un rôle pionnier dans le cadre des différents travaux multilatéraux. Ces travaux ont permis de faire émerger un cadre pour le comportement responsable des États dans leur usage des TIC. Ce cadre est fondé sur le droit international, sur un ensemble cohérent de normes de comportement non contraignantes et sur des mesures de transparence et de confiance. Il permet de faire progresser la coopération et la compréhension mutuelle entre États dans le cyberespace. Je souhaite saluer les succès récents du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et du sixième Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui ont adopté deux rapports équilibrés, utiles et consensuels. La France est prête à continuer de participer de façon constructive aux discussions multilatérales au sein des Nations Unies, y compris dans le cadre du nouveau Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) créé en vertu de la résolution 75/240 de l'Assemblée générale.

Il convient surtout désormais de mettre en pratique concrètement les normes et principes agréés. La France, avec 52 partenaires, propose la création d'un Programme d'action sur la cybersécurité, dans le cadre des Nations Unies. Ce nouvel outil, complémentaire du nouveau groupe de travail permettra de créer une structure pérenne. Elle aura vocation à soutenir le renforcement des capacités et à créer des espaces de dialogue avec la société civile, les chercheurs et les acteurs privés. La France est ouverte au dialogue avec l'ensemble des États et des parties prenantes intéressées pour préciser et construire cette proposition orientée vers l'action.

Cet engagement collectif, multi-acteurs, est essentiel. Dans le cyberespace, les États ont certes des responsabilités qu'aucun autre acteur ne peut prétendre assumer, mais ils ne peuvent agir seuls. Nous devons nous lancer pleinement dans cette nouvelle forme de diplomatie.

Annexe XIII

Déclaration du Représentant permanent de la Chine, M. Zhang Jun

[Original : chinois]

Il se produit, de nos jours, un nouveau cycle de révolution technologique et de transformation industrielle et les technologies numériques et les cybertechnologies, qui évoluent rapidement, modifient considérablement les modes de production et les modes de vie et stimulent le développement économique et social dans tous les pays. Dans le même temps, la cybersurveillance, les cyberattaques, la cybercriminalité et le cyberterrorisme sont devenus des menaces généralisées à l'échelle mondiale, tandis que le cyberespace est de plus en plus militarisé, politisé, insécurisé et idéologisé. Dans le cyberespace, les pays partagent non seulement des perspectives et des intérêts mais aussi des contraintes et des responsabilités. Ils constituent de plus en plus une communauté de destin, dont le cheminement connaît des hauts et des bas.

Le président chinois Xi Jinping a déclaré que, bien que les pays diffèrent de par leur situation et l'état de développement de l'Internet et qu'ils affrontent des problèmes différents, ils partagent le même désir de faire progresser l'économie numérique, le même intérêt à surmonter les problèmes de la cybersécurité et le même besoin de renforcer la gouvernance du cyberespace. La Chine a toujours appelé la communauté internationale à œuvrer de concert en vue d'assurer la cybersécurité et de préserver la paix dans le monde.

- Nous devons promouvoir la sécurité en préservant la paix et en évitant que le cyberespace ne devienne un nouveau champ de bataille. La communauté internationale doit se conformer aux buts et principes consacrés par la Charte des Nations Unies, notamment ceux ayant trait à l'égalité souveraine des États, à l'interdiction du recours à la force, à la non-ingérence dans les affaires intérieures d'autres États et au règlement pacifique des différends. Il importe tout particulièrement de respecter le droit de chaque pays de choisir, en toute indépendance, le mode de développement de son réseau et le système de gestion de ce dernier et de participer à la gouvernance du cyberespace sur un pied d'égalité. Les pays doivent s'abstenir d'entreprendre des cyberactivités qui mettent en danger la sécurité d'autres pays. Il convient de faire preuve de prudence en ce qui concerne l'application du droit des conflits armés au cyberespace et de faire obstacle à la course aux armements dans ce domaine.

- Nous devons promouvoir la sécurité par les échanges et la coopération et créer un environnement propice au sein du cyberespace. La protection de la cybersécurité est un enjeu mondial et aucun pays ne peut s'en désintéresser ou y faire face seul. L'hégémonisme, l'unilatéralisme et le protectionnisme dans le cyberespace, qui ne peuvent qu'intensifier les confrontations et empoisonner le climat de coopération, devraient être rejetés et combattus de front par la communauté internationale. Les pays devraient œuvrer de concert pour approfondir les échanges et la coopération en matière de recherche-développement dans le domaine de la technologie, d'élaboration de règles et de partage d'informations et devraient s'employer conjointement à enrayer l'utilisation abusive de la technologie de l'information. Nous devons lutter ensemble contre la cybersurveillance, les cyberattaques, le cyberterrorisme et la cybercriminalité et renforcer les capacités de protection de la cybersécurité. Il est essentiel d'offrir aux entreprises un environnement commercial ouvert, équitable et non discriminatoire, de garantir l'ouverture, la stabilité et la sécurité des chaînes d'approvisionnement de l'industrie mondiale des technologies de l'information, de promouvoir le développement sain de l'économie mondiale et

de s'opposer à l'ingérence humaine dans les opérations commerciales normales des entreprises, quel qu'en soit le prétexte.

- Nous devons promouvoir la sécurité par une meilleure gouvernance et promouvoir l'équité et la justice dans le cyberespace. Tous les pays doivent défendre un multilatéralisme effectif, établir un processus de gouvernance de la cybersécurité ouvert, inclusif et durable dans le cadre de l'Organisation des Nations Unies et avec la participation égale de tous, formuler des règles internationales pour le cyberespace, qui soient généralement acceptées par tous, et s'opposer aux chapelles et au sectarisme. La Chine se félicite vivement de l'achèvement des rapports sur la cybersécurité du Groupe de travail à composition non limitée des Nations Unies et du Groupe d'experts gouvernementaux et attend avec intérêt les conclusions du nouveau Groupe de travail à composition non limitée relatives à la cybersécurité. Nous sommes disposés à coopérer avec toutes les parties afin de promouvoir, dans le cadre des Nations Unies, l'élaboration d'une convention internationale contre la cybercriminalité. Il convient de valoriser pleinement le rôle des différentes parties prenantes, telles que les gouvernements, les entreprises de l'Internet, les communautés technologiques, la société civile et les citoyens individuels, en procédant à des consultations approfondies, en effectuant des contributions conjointes et en mutualisant les avantages.

- Nous devons promouvoir la sécurité par un développement inclusif et parvenir à une prospérité partagée dans le cyberespace. Le développement économique mondial actuel est à la traîne. Les technologies numériques et cybernétiques peuvent contribuer, dans une large mesure, à promouvoir le relèvement des pays et la relance de leur développement économique et social après la pandémie. Les pays devraient adopter des politiques plus proactives, globales, coordonnées et inclusives pour promouvoir le développement équilibré des technologies de l'information et des communications à l'échelle mondiale, mettre au point de nouveaux modèles et de nouveaux formats tels que l'économie numérique, et faire obstacle aux tentatives d'hégémonie scientifique et technologique. Nous devons promouvoir le développement de l'infrastructure et de la connectivité numériques, faire tomber les barrières de l'information, réduire la fracture numérique et aider les pays en développement à relever leur niveau de numérisation, de connectivité et de développement des connaissances, aux fins de la mise en œuvre du Programme de développement durable à l'horizon 2030. Nous devons renforcer la coopération avec les pays en développement et l'aide qui leur est apportée dans le domaine de la cybersécurité et améliorer leurs capacités d'alerte précoce, de prévention et d'intervention d'urgence en cas de cyberincidents.

La Chine attache une grande importance à la cybersécurité et à l'informatisation et tient à construire une économie numérique, une société numérique et un gouvernement numérique, en utilisant la transformation numérique globale pour induire des changements dans les modes de production, les modes de vie et les systèmes de gouvernance. La Chine continuera à améliorer ses lois, ses réglementations et ses normes institutionnelles nationales en matière de cybersécurité, en s'appuyant sur la Loi relative à la cybersécurité et la Loi relative à la sécurité des données.

L'année dernière, la Chine a présenté l'initiative mondiale sur la sécurité des données, qui se concentre sur des questions telles que les infrastructures critiques et la protection des informations personnelles, le stockage et la récupération des données pour les entreprises étrangères et la sécurité de la chaîne d'approvisionnement, en proposant des solutions constructives destinées à préserver la cybersécurité et les

données à l'échelle mondiale. Récemment, la Chine a publié, en collaboration avec la Ligue des États arabes (LEA), l'initiative de coopération Chine-LEA sur la sécurité des données, qui concrétise l'appel conjoint des deux parties en faveur du maintien de la cybersécurité et de la sécurité des données. Nous nous félicitons des réponses et de la participation de toutes les parties à l'initiative, qui permettront de formuler conjointement des règles mondiales pour la gouvernance numérique. Par ailleurs, la Chine poursuit activement la construction de la Route de la soie numérique, en collaborant avec d'autres pays pour mettre en place un nouveau modèle d'interconnexion intelligente tourné vers l'avenir.

Le cyberespace incarne le rêve de l'humanité, qui embrasse le bien-être, la paix et la sécurité des personnes. La Chine est disposée à coopérer avec tous les pays en vue de saisir l'occasion offerte par la révolution de l'information pour favoriser un nouvel élan en faveur de l'innovation et du développement, mettre en place un nouvel environnement pour la coopération numérique, forger un nouveau modèle de cybersécurité, construire une communauté à l'avenir partagé dans le cyberespace et créer conjointement un meilleur avenir pour l'humanité.

Annexe XIV

Déclaration de la Mission permanente du Mexique auprès de l'Organisation des Nations Unies

[Original : espagnol]

Le Mexique se félicite de l'organisation du présent débat public et apprécie l'exposé de la Secrétaire générale adjointe et Haute Représentante pour les affaires de désarmement, M^me^ Izumi Nakamitsu.

Comme nous l'avons entendu ici et dans de nombreuses autres instances, l'importance croissante du cyberespace est désormais incontestable. Le monde est devenu de plus en plus dépendant des technologies de l'information et des télécommunications, notamment à la faveur de la pandémie. Les relations internationales ont elles aussi rapidement évolué vers le domaine virtuel et le Conseil de sécurité ne peut pas et ne doit pas être indifférent aux conséquences de ce phénomène en ce qui concerne la paix et la sécurité internationales.

Même si près de la moitié de la population mondiale n'a pas accès à l'Internet, elle n'en reste pas moins exposée à l'une ou l'autre de ces milliers de cyberattaques qui, quotidiennement, visent les réseaux gouvernementaux, les institutions bancaires ou financières, les instituts de recherche et même les établissements de santé.

Ces risques latents ont conduit divers organes du système des Nations Unies à se pencher sur les menaces et à rechercher des accords entre les États, afin de garantir que le cyberespace n'est pas utilisé à des fins criminelles, hostiles ou même terroristes, sans perdre de vue l'équilibre avec les utilisations pacifiques et les possibilités considérables qu'offre le cyberespace en matière de développement durable.

Le Mexique estime qu'il est essentiel de prévenir toute escalade des risques liés à la cybersécurité. L'utilisation du cyberespace, comme de tout autre domaine physique, devrait être réglementée par des principes directeurs et des paramètres clairs, et il convient de contribuer à la promotion d'un cyberespace ouvert, libre, sûr, sécurisé, stable, accessible et résilient.

Le Mexique se félicite donc de l'aboutissement des travaux du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée, qui ont permis l'adoption de rapports de fond par consensus, lesquels constituent des précédents importants pour l'action multilatérale. Pour mon pays, il s'agit d'une réaffirmation de la confiance qui prévaut vis-à-vis du multilatéralisme et du rôle constructif que joue l'ONU dans la recherche de solutions globales, légitimes et de long terme aux problèmes que posent le cyberespace et les technologies de l'information et des télécommunications.

Mais, cela ne suffit pas. Il faut progresser dans l'application intégrale du droit international dans le cyberespace, y compris non seulement la Charte des Nations Unies mais aussi le droit international des droits de l'homme, le droit international humanitaire et le développement de la jurisprudence en vertu de ceux-ci.

Notre démarche s'inscrit dans un processus fondé sur une amélioration de la transparence des activités dans le cyberespace, l'application du principe de responsabilité et la mise en œuvre des normes de comportement responsable des États, adoptées par l'Assemblée générale, le tout complété par des mesures destinées à promouvoir la coopération internationale dans les domaines de la mise en place et du renforcement des cybercapacités des États.

Le Mexique espère que, dans ses délibérations et travaux futurs, le Conseil de sécurité se fera l'écho des voix de plus en plus audibles de la société civile, des milieux universitaires et du secteur privé, qui visent à juste titre un objectif commun : garantir une utilisation pacifique du cyberespace pour le développement et l'utilisation des technologies numériques.

Annexe XV

Déclaration du Représentant permanent de la Fédération de Russie auprès de l'Organisation des Nations Unies, M. V. A. Nebenzia

[Original : russe]

L'année qui a suivi le déclenchement de la pandémie de maladie à coronavirus (COVID-19) a été, pour le monde entier, une période de grandes épreuves, qui restera dans les mémoires surtout comme une année de difficultés et de manque à gagner. De nombreuses démarches diplomatiques ont été émaillées de difficultés et les négociations se sont enlisées sur de nombreux fronts.

Les discussions multilatérales sur la sécurité internationale de l'information à l'ONU se distinguent à cet égard, puisqu'elles ont non seulement conservé leur élan, mais également donné des résultats, si j'ose dire, historiques. Les deux forums d'experts désignés par l'Assemblée générale des Nations Unies, à savoir le Groupe d'experts gouvernementaux et le Groupe de travail à composition non limitée, ont pu adopter leurs rapports finals par consensus.

Les négociations au sein de ces groupes n'ont pas été faciles, ce qui rend d'autant plus appréciables les résultats durement acquis. Ces résultats ont clairement montré que la communauté internationale est capable de s'accorder sur des questions clés lorsque le dialogue est pragmatique, dépolitisé et constructif. Grâce à ces travaux, nous abordons maintenant une nouvelle phase importante, qui a débuté en juin 2021 avec la session d'organisation du nouveau Groupe de travail à composition non limitée pour 2021-2025.

Ce résultat est une réalisation commune de la communauté internationale. Pour notre part, nous nous efforçons depuis des décennies de contribuer à la mise en place d'un système mondial permettant d'assurer la sécurité internationale de l'information. En 1998, la Russie a fait état, pour la première fois à l'ONU, de la nécessité de s'attaquer aux menaces qui pèsent sur la sécurité de l'information internationale et proposé une résolution de l'Assemblée générale à cet effet. Au début des années 2000, nous avons proposé la création du Groupe d'experts gouvernementaux, qui devait constituer un forum d'experts chargé d'examiner la question de la sécurité internationale de l'information. En 2019, lorsqu'il est apparu clairement que la question avait dépassé le cadre étroit du Groupe, nous avons entrepris, avec des délégations partageant les mêmes idées, de répondre aux besoins de la communauté internationale en lançant le processus de négociation ouvert et démocratique sur la sécurité internationale de l'information, ouvert à la participation de tous les États membres, sous le format « Groupe de travail à composition non limitée ».

Il s'agissait là d'un tournant important. Pour la première fois, les discussions relatives à la sécurité numérique étaient ouvertes à la majorité des États Membres de l'ONU. Notre position est très simple : nous croyons en un dialogue fondé sur l'égalité et le respect mutuel. Si nous sommes tous égaux face aux menaces qui pèsent sur la sécurité internationale de l'information, ces menaces doivent être discutées non pas par un cercle limité d'États technologiquement avancés mais par tous les États Membres de l'ONU. Les États qui se considèrent comme étant plus « avancés » ne devraient pas imposer leur volonté.

Nos propositions relatives à la création du Groupe d'experts gouvernementaux et, plus tard, du Groupe de travail à composition non limitée n'ont pas été du goût de tous dans un premier temps. Plusieurs États, y compris des États qui participent à la réunion d'aujourd'hui, ont voté contre leur création. Toutefois, ils ont

progressivement commencé à se joindre à la conversation, pour finalement devenir des participants actifs et constructifs.

Une diplomatie multilatérale efficace dans le domaine de la sécurité internationale de l'information à l'ONU, qui complète la coopération bilatérale entre les États sur ce sujet, constitue une excellente illustration de la manière dont il convient d'aborder ces questions pour surmonter la méfiance mutuelle et dissiper les inquiétudes. Cette démarche contraste avec la fameuse « diplomatie du mégaphone » à laquelle, malheureusement, certains de nos partenaires ont parfois recours.

Dans le même temps, nous sommes malheureusement témoins d'une tendance dangereuse du Conseil de sécurité de l'ONU, qui consiste à tenter d'imposer des interprétations unilatérales des accords conclus au sein du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée, et, ainsi, à demander effectivement que les résultats des discussions de ces forums désignés par l'Assemblée générale soient soutenus ou, pire encore, révisés. Nous estimons que de telles tentatives sont destructrices. Elles poussent la communauté internationale vers des confrontations imprévisibles et malvenues.

Plus précisément, en altérant les accords, notamment sur les aspects juridiques internationaux de l'utilisation des technologies de l'information et des communications (TIC), certains pays cherchent à justifier des pressions et des sanctions unilatérales contre d'autres États Membres et un éventuel recours à la force contre eux. Il est très préoccupant que plusieurs États technologiquement avancés s'emploient activement à militariser l'espace de l'information en mettant en avant le concept de « cyberattaques militaires préventives », y compris contre des infrastructures critiques. Ces doctrines conflictuelles sont en contradiction avec l'engagement qu'ils ont pris, y compris aujourd'hui, de prévenir les conflits découlant de l'utilisation des TIC. Il s'agit d'une tentative d'utiliser leur position de force pour imposer leurs propres « règles du jeu » dans la sphère de l'information.

Je tiens à souligner que, si le secteur numérique n'est pas sans réglementation, le débat sur la manière exacte dont le droit international peut lui être appliqué est loin d'être clos. Cette question seront débattues pendant encore au moins cinq années au sein du forum désigné par l'Assemblée générale – le nouveau Groupe de travail à composition non limitée.

À cet égard, les rapports finals du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée constituent un ensemble d'accords équilibrés et précis, notamment en ce qui concerne la nécessité d'élaborer de nouvelles normes pour un comportement responsable des États dans l'espace de l'information, en tenant compte de ses particularités. La liste initiale de ces règles a été inscrite dans la résolution concernant la sécurité internationale de l'information, adoptée par l'Assemblée générale en 2018 à l'initiative de la Fédération de Russie. Il est regrettable que nos collègues occidentaux tentent aujourd'hui de choisir dans cette liste les dispositions qui leur sont le plus profitables, tout en interprétant à tort l'applicabilité du droit international dans la sphère numérique comme étant « automatique », ce qui autoriserait le recours à la force dans ce domaine, et en présentant leurs points de vue nationaux comme s'agissant du fruit d'un consensus mondial. Nous nous opposerons donc à toute tentative de réviser, par le truchement du Conseil de sécurité de l'ONU, les accords équilibrés conclus dans les forums désignés par l'Assemblée générale.

Comme l'a déclaré le Président de la Fédération de Russie, V. Poutine, lors de la réunion du Conseil de sécurité de la Fédération de Russie, le 26 mars 2021, les approches doctrinales russes concernant l'élaboration d'un système mondial visant à assurer la sécurité internationale de l'information restent ouvertes, transparentes et

inchangées. Elles sont inscrites dans les Principes fondamentaux de la politique de l'État concernant la sécurité de l'information internationale, approuvés par le Président en avril 2021. Il s'agit d'un document public, que j'encourage tout un chacun à lire.

Notre doctrine repose sur le principe de l'utilisation des TIC uniquement à des fins pacifiques et sur la nécessité de prévenir les conflits dans l'espace de l'information et de renforcer la coopération multilatérale et bilatérale à cette fin. Nous estimons qu'il y a lieu de conclure des accords juridiques internationaux universels pour pouvoir aborder ces tâches de manière effective. Pour atteindre cet objectif, il convient de prendre des initiatives communes pour : élaborer et adopter d'un commun accord des règles universelles, équitables et complètes concernant le comportement des États dans l'espace de l'information, qui tiennent compte des réalités actuelles différencier clairement les activités qui sont autorisées et celles qui ne le sont pas dans l'espace de l'information rendre ces règles juridiquement contraignantes afin d'en garantir le respect strict par tous les États.

Parallèlement, nous défendons l'inviolabilité de la souveraineté des États dans la sphère numérique. Il appartient à chaque pays de déterminer les paramètres de la réglementation de son propre espace d'information et de l'infrastructure connexe.

Une tâche tout aussi importante consiste à mettre en place un système pacifique, équitable et juste, qui permette d'assurer la sécurité internationale de l'information et tienne compte des intérêts de tous les pays, quel que soit leur potentiel numérique. Les initiatives dirigées par l'ONU et qui visent à renforcer ces capacités en vue de réduire la fracture numérique devraient être résolument soutenues. Nous espérons bien que le nouveau Groupe de travail à composition non limitée pourra, conformément à son mandat, continuer à examiner cette question de manière approfondie et à formuler des recommandations pertinentes.

D'autre part, nous devons collectivement lutter contre l'utilisation des TIC à des fins criminelles. Nous appelons les États membres à contribuer de manière constructive aux travaux du comité spécial chargé d'élaborer un projet de convention sur la question d'ici à 2023.

L'Assemblée générale reste la principale instance à même d'examiner la question de la sécurité internationale de l'information. C'est au sein de cette instance que les débats d'experts sur tous les aspects de cette question se tiendront au cours des cinq prochaines années. Nous devons nous attacher à soutenir ce processus unique. Nous devons préserver l'atmosphère constructive de la coopération multilatérale en matière de sécurité internationale de l'information sous les auspices de l'ONU, sous le format du Groupe de travail à composition non limitée, qui a réellement démontré son efficacité et sa pertinence. Le nouveau Groupe de travail à composition non limitée pourra ainsi, véritablement, obtenir des résultats concrets et pratiques. Il est de notre devoir commun, en tant que membres du Conseil de sécurité de l'ONU, de contribuer activement à cette entreprise.

Annexe XVI

Déclaration de M. Tarek Ladeb, Représentant permanent de la Tunisie auprès de l'Organisation des Nations Unies

Je voudrais tout d'abord remercier la présidence estonienne d'avoir organisé cette réunion sur la cybersécurité et le maintien de la paix et de la sécurité internationales dans le cyberespace.

Je remercie la Secrétaire générale adjointe et Haute-Représentante pour les affaires de désarmement, M^me^ Nakamitsu, de son exposé substantiel.

La Tunisie est profondément préoccupée par l'augmentation significative, ces dernières années, des activités malveillantes dans le cyberespace qui peuvent constituer une menace sérieuse pour la paix et la sécurité internationales, en particulier lorsque des infrastructures critiques sont visées.

De nombreux États ont également développé ouvertement des cybercapacités à des fins militaires, un phénomène qui peut déclencher une course aux cyberarmes et accroître encore le nombre de cyberattaques et de contre-attaques ainsi que les risques d'erreurs de jugement pouvant déboucher sur un conflit armé.

La Tunisie est également préoccupée par le fait que les cybercapacités, auxquelles seuls les États avaient accès auparavant, sont maintenant accessibles à des acteurs non étatiques, y compris des organisations terroristes, qui s'en servent avec l'intention de nuire. Ces capacités seraient souvent volées à des entités gouvernementales ou acquises de sources non autorisées, ce qui soulève encore la question de la responsabilité des États.

L'éventualité que des groupes terroristes lancent des cyberattaques dévastatrices contre des infrastructures critiques, comme les centrales nucléaires, ne peut plus être écartée et devrait être prise au sérieux.

La Tunisie réaffirme le bien-fondé de l'application du droit international en ce qui concerne l'utilisation des technologies numériques par les États, et souligne à cet égard qu'il importe de respecter les principes consacrés par la Charte des Nations Unies, notamment le règlement des différends internationaux par des moyens pacifiques, le renoncement à la menace ou à l'emploi de la force et le respect des droits humains et des libertés fondamentales.

Nous tenons également à rappeler le bien-fondé de l'application du droit international humanitaire aux cyberopérations menées pendant les conflits armés.

Ma délégation se félicite de l'adoption par consensus, au début de l'année, des rapports du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et du Groupe d'experts gouvernementaux sur la promotion d'un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, qui ont tous les deux permis aux États Membres d'avoir une meilleure compréhension de la manière dont le droit international s'applique et leur ont donné des orientations supplémentaires sur la manière dont des normes volontaires et non contraignantes peuvent également jouer un rôle important dans la prévention des conflits et la promotion d'un cyberespace ouvert, sûr, stable, accessible et pacifique.

Nous espérons qu'il y aura des discussions ouvertes et inclusives sur la cybersécurité lors des sessions du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), nouvellement constitué, afin

de renforcer la capacité de tous les États à prévenir ou à atténuer les effets des cyberactivités malveillantes, des cybermenaces et des cyberattaques.

Pour sa part, sous la supervision de son Conseil de sécurité nationale et avec la participation du secteur privé et de la société civile, la Tunisie a adopté en octobre 2019 une stratégie nationale de cybersécurité dont l'objectif est d'améliorer la résilience du pays face aux cybermenaces par le renforcement de ses capacités, de son système juridique, dans le respect strict des droits et libertés fondamentaux, et de la coopération internationale.

Enfin, étant donné que les systèmes du cyberespace sont liés les uns aux autres, nous pensons que la mise en commun d'informations sur les faiblesses constatées et le renforcement des capacités des acteurs qui en font la demande sont d'une importance cruciale pour la réduction des risques que les cybermenaces font peser sur la paix et la sécurité internationales.

Annexe XVII

Déclaration de la Mission permanente de l'Argentine auprès de l'Organisation des Nations Unies

[Original : espagnol]

L'Argentine remercie l'Estonie d'avoir pris l'initiative d'organiser un débat public afin de contribuer à une meilleure compréhension des risques croissants découlant des activités malveillantes dans le cyberespace et de leurs effets sur la paix et la sécurité internationales. Le Conseil de sécurité, de par son mandat et sa nature, permet de donner à cette question toute la pertinence et toute l'importance qu'elle revêt.

Le nombre régulier et croissant d'actes de cybermalveillance graves émanant de différentes parties du monde est un signal d'alarme permanent pour tous sur la nécessité de continuer à mieux comprendre la gestion de ces actes, dont certains peuvent compromettre la paix et la sécurité internationales, de créer des cadres de coopération et de favoriser le renforcement des capacités des pays à faire face à ces problèmes qui touchent l'ensemble de la communauté internationale. Cela nécessite des actions multiples aux niveaux national, régional et international.

Au niveau international, et dans le but d'aborder l'un des aspects les plus critiques de la question, l'Argentine considère qu'il importe au plus haut point de maintenir des espaces larges et inclusifs dans lesquels les pays de toutes les régions peuvent s'engager de manière active, avec des visions diverses, l'objectif étant de parvenir à un consensus sur les règles, les normes et les principes de comportement responsable des États et la manière dont le droit international s'applique dans le cyberespace, entre autres aspects. L'Argentine comprend qu'il existe un important corpus de normes, règles et principes volontaires qui ont été acceptés par consensus par tous les membres de l'Assemblée générale pour régir l'utilisation par les États des technologies numériques et définir le comportement responsable des États dans le cyberespace, et qui sont essentiels pour le maintien de l'utilisation pacifique et de la stabilité du cyberespace. Ce corpus est un point de départ et une base qui doit être préservée et développée.

À ce propos, nous attachons une valeur particulière au consensus obtenu dans le cadre du premier Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui s'appuie sur ces principes ouverts. Nous accordons également une attention particulière au rapport du dernier 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. Il est intéressant de noter que les deux groupes ont publié des rapports de consensus cette année, avec des recommandations et des contributions importantes pour la poursuite des efforts visant à parvenir au consensus déjà obtenu dans le passé.

Il importe au plus haut point d'assurer la continuité d'un cadre de discussion ouvert, inclusif et tourné vers l'avenir, le but étant de consolider davantage les accords conclus et de réaliser de nouveaux progrès. Nous saluons donc la création d'un nouveau Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, dont le mandat dure jusqu'en 2025, auquel notre pays continuera de prendre une part active et dans un esprit constructif.

Dans le même ordre d'idées et avec une approche plus efficace, l'Argentine, se joignant à un nombre important de pays de toutes les régions, soutient l'initiative internationale appelée programme d'action sur les progrès de l'informatique et des

télécommunications dans le contexte de la sécurité internationale. Ce programme d'action, qui est en pleine étude théorique, propose un schéma de discussion ouvert, inclusif, flexible et permanent, sous les auspices de l'ONU, dirigé par les États et avec une participation significative de tous les acteurs impliqués dans le cyberespace. Nous invitons tous les pays à s'intéresser à cette initiative.

L'Argentine considère que la protection et la défense des droits humains et des libertés fondamentales consacrés par la Charte des Nations Unies et par les traités internationaux doivent sous-tendre notre vision. La question du genre et la protection particulière des groupes vulnérables doivent également être prises en compte dans toutes les actions que nous entreprenons.

Dans un contexte d'innovations continues dans le domaine du numérique, il est nécessaire d'œuvrer activement pour que toutes les nations puissent bénéficier des avantages de ces technologies de manière équitable et équilibrée. Nous pensons donc que la question de la réduction de la fracture numérique entre les États et à l'intérieur de ceux-ci devrait être constamment examinée dans ce débat.

Cet examen va de pair avec le renforcement des capacités des pays. Les possibilités de travail sur cet aspect sont énormes et l'une des principales consiste à développer des synergies avec les autres acteurs impliqués dans le cyberespace, tels que le secteur privé, la société civile, les milieux universitaires et le secteur technique.

Les organisations régionales et sous-régionales se sont avérées être des acteurs importants et décisifs en tant que catalyseurs pour le renforcement des capacités des pays, la promotion de visions communes et la facilitation de la coopération internationale.

Il ne fait aucun doute que les États doivent déployer des efforts considérables au niveau national, mettre en place des capacités, des structures et des normes efficaces, en accordant à cette question l'importance et la priorité voulues.

Nous espérons que ce débat nous permettra de définir de nouveaux modes de compréhension qui contribueront à rendre le cyberespace libre, ouvert, sécurisé, interopérable et stable.

Annexe XVIII

Déclaration de M. Mitchell Fifield, Représentant permanent de l'Australie auprès de l'Organisation des Nations Unies

L'Australie remercie l'Estonie de lui avoir donné de l'occasion de faire une déclaration au Conseil de sécurité sur la paix et la sécurité internationales dans le cyberespace. À mesure que l'importance stratégique du cyberespace augmente, de plus en plus de groupes tenteront d'y exercer leur pouvoir. Les questions numériques sont devenues des questions stratégiques de politique étrangère qui sont une source de grande préoccupation pour tous les pays, et il est essentiel que ces questions soient considérées comme telles par la communauté internationale.

Certes la fréquence, l'ampleur, la complexité et la gravité des actes de cybermalveillance ne cessent d'augmenter, mais l'ONU a toujours encouragé la coopération internationale pour comprendre ces menaces et promouvoir un cyberespace ouvert, libre, sûr, interopérable et pacifique.

Tous les membres de l'ONU s'accordent à estimer, à l'unanimité, que le droit international existant, en particulier la Charte des Nations Unies dans son intégralité, est applicable dans le cyberespace et essentiel au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement ouvert, sûr, stable, accessible et pacifique en matière d'informatique et de technologies des communications[3].

L'Australie a exprimé son point de vue sur la manière dont certains principes du droit international s'appliquent au comportement des États dans le cyberespace (2017, 2019 et 2021) et publié des études de cas juridiques fictives (2020)[4].

Le droit international humanitaire, notamment les principes d'humanité, de nécessité, de proportionnalité et de distinction, s'applique aux cyberactivités en situation de conflit armé. Le droit international humanitaire prévoit des règles qui s'appliquent aux cyberactivités dans un conflit armé qui ne constituent pas une « attaque » ou qui ne peuvent pas être qualifiées comme telle, y compris les protections générales accordées à la population civile et aux personnes civiles contre les dangers découlant des opérations militaires.

Le droit international des droits humains s'applique également au comportement des États dans le cyberespace. En vertu du droit international des droits de l'homme, les États ont l'obligation de protéger les droits humains pertinents des personnes relevant de leur juridiction, notamment le droit à la vie privée, lorsque ces droits sont exercés dans le cyberespace ou en se servant de celui-ci.

Reconnaissant les caractéristiques atypiques du cyberespace, tous les États Membres ont accepté en 2015 de fonder leur utilisation de l'informatique et des communications sur 11 normes facultatives et non contraignantes de comportement responsable des États dans le cyberespace[5]. Ces normes complètent les obligations légales actuelles des États, mais ne se substituent pas à celles-ci. Collectivement, le droit international et les normes internationales fixent des attentes claires en matière de comportement responsable des États, et favorisent ainsi la prévisibilité, la stabilité et la sécurité.

Tous les États ont également reconnu la nécessité d'adopter des mesures de confiance et de mener des activités coordonnées de renforcement des capacités[6]. Les

---

[3] Voir les résolutions 68/243 et 70/237 et la décision 75/564 de l'Assemblée générale.

[4] Voir : www.internationalcybertech.gov.au/international-security-at-the-un.

[5] Voir la résolution 70/237 de l'Assemblée générale.

[6] Ibid.

mesures de confiance, conçues en vue d'éviter les malentendus qui conduisent à des conflits, sont aujourd'hui plus importantes que jamais, et il est nécessaire de mener des activités ciblées de renforcement des capacités pour que tous les pays soient en mesure de relever les défis et de profiter des possibilités qu'offre une connectivité accrue.

Collectivement, ces mesures (le droit international, les normes, les mesures de confiance et le renforcement des capacités) jettent les bases d'un cyberespace sûr, stable et prospère et sont souvent appelées le cadre des Nations Unies de comportement responsable des États (ci-après dénommé le Cadre). Les éléments du Cadre se renforcent mutuellement et aucun d'entre eux ne doit être considéré isolément.

Le fait que Cadre est universellement accepté[7] par tous les États Membres représente un progrès important dans la promotion de la paix et de la stabilité internationales dans le cyberespace. Si le Cadre est scrupuleusement respecté, il constitue une base solide pour faire face aux menaces que représente la cyberactivité malveillante provoquée ou parrainée par des États.

L'Australie réaffirme son engagement à agir conformément au Cadre de comportement responsable des États dans le cyberespace, tel que défini dans les rapports cumulatifs des groupes d'experts gouvernementaux en 2010, en 2013, en 2015 et en 2021[8], et dans le rapport 2021 du Groupe de travail à composition non limitée[9], et invite tous les pays à faire de même.

Cependant, un petit nombre d'acteurs étatiques et d'acteurs parrainés par des États font de plus en plus fi du droit international et des normes internationales, malgré les attentes clairement fixées par la communauté internationale. En agissant de la sorte, ils menacent la paix et la stabilité internationales.

Nous n'avons besoin ni de règles supplémentaires ni de nouvelles règles, mais plutôt que les règles déjà acceptées soient respectées et que l'obligation de rendre compte soit mieux appliquée lorsque celles-ci sont violées. Pour lutter contre les activités malveillantes, nous devons prévoir des mesures efficaces à l'égard de ceux qui contreviennent au droit international en vigueur et aux normes adoptées d'un commun accord en matière de comportement responsable des États.

L'Australie s'engage à contrer, à dissuader et à prévenir la cybermalveillance, en particulier celle des États et de leurs mandataires. L'Australie travaillera avec ses partenaires pour renforcer les actions coordonnées face aux comportements inacceptables dans le cyberespace. La lutte contre les activités malveillantes protège la stabilité internationale. L'objectif de la politique australienne de lutte contre les cyberactivités malveillantes est de prévenir les actes de cybermalveillance majeurs qui portent atteinte aux intérêts de l'Australie et de ses partenaires internationaux.

Une coopération efficace entre les États et la communauté multipartite (notamment la société civile, le secteur privé, les milieux universitaires et les spécialistes techniques) a des effets concrets sur la sécurité, renforce les capacités et crée un cycle de développement, d'ouverture et de stabilité dans le cyberespace. Souvent les premières victimes des actes de cybermalveillance, les protecteurs des infrastructures critiques, les bienfaiteurs et les bénéficiaires de l'expertise technique, ainsi que les capitaux fluctuants d'acteurs non étatiques du cyberespace sont autant de raisons supplémentaires d'assurer un environnement pacifique en ligne.

---

[7] Décision 75/564 de l'Assemblée générale ; A/75/816.
[8] A/65/201, A/68/98 et A/70/174.
[9] A/75/816.

L’inégalité de genre est un obstacle à la paix, à la stabilité et à la sécurité mondiales dans le cyberespace. Elle est une des causes de toute une série de problèmes, dont la pauvreté, la mauvaise gouvernance, les conflits et l’extrémisme violent, et les aggrave souvent. La valeur de l’égalité des genres et de la participation des femmes à la prise de décision, aux rôles de premier plan et aux efforts de consolidation de la paix liés à la paix et à la sécurité internationales dans le cyberespace est indiscutable. L’Australie continuera de promouvoir, par l’adoption de mesures concrètes, la participation active et effective des femmes dans tous les espaces de discussions relatives à la paix et à la sécurité internationales dans le cyberespace.

Les cyberactivités malveillantes peuvent causer des dégâts ou des perturbations considérables et de tels événements sont de plus en plus nombreux. Le fait que la communauté internationale s’intéresse de plus en plus à ces questions et y est de plus en plus attentive constitue une occasion qu’il ne faut pas laisser passer. Il faut saisir cette occasion afin de mieux comprendre la manière dont le droit international s’applique dans le cyberespace, de promouvoir l’application concrète des normes relatives au comportement responsable des États et des mesures de confiance, de coordonner les activités de renforcement des capacités, le but étant de faire en sorte que tous les pays comprennent et puissent mettre en œuvre le Cadre et de permettre l’expression d’une diversité de voix.

Annexe XIX

Déclaration de la Mission permanente de l'Autriche auprès de l'Organisation des Nations Unies

L'Autriche remercie l'Estonie, qui assure la présidence du Conseil de sécurité pour le mois de juin 2021, d'avoir organisé ce débat public sur la paix et la sécurité internationales dans le cyberespace. L'Autriche souscrit à la déclaration de l'Union européenne. À titre national, nous tenons à ajouter les observations ci-après.

Aujourd'hui, c'est la première fois que le Conseil de sécurité aborde de manière distincte la question de la cybersécurité : il s'agit d'une évolution opportune. Afin de rester pertinent et de s'acquitter de son mandat, le Conseil de sécurité doit absolument continuer de lutter contre les menaces contemporaines contre la paix et la sécurité internationales.

Les cyberactivités malveillantes, qui sont de plus en plus nombreuses, ont multiplié les menaces dans le cyberespace au cours des dernières années. Dans le monde interconnecté d'aujourd'hui, où les infrastructures dépendent de plus en plus des systèmes de régulation numérique, les effets des cyberattaques peuvent être les mêmes que ceux des attaques conventionnelles et parfois ils peuvent être plus graves. Ces évolutions, associées aux difficultés de connaître les auteurs des cyberattaques, font monter l'insécurité, et augmentent le risque d'erreurs de jugement et le risque d'erreur humaine lorsqu'il s'agit de décider de la riposte à donner à une attaque subie.

Si le cyberespace diffère du monde réel dans son fonctionnement, on ne peut se méprendre sur un fait simple : le droit international dans son intégralité s'applique pleinement dans le cyberespace aussi. Cela a été confirmé, tout récemment, par les résultats des travaux du Groupe de travail à composition non limitée sur l'informatique et les communications et du Groupe d'experts gouvernementaux sur la cybersécurité, qui ont tous les deux adopté par consensus d'importants documents finals permettant de mieux comprendre les problèmes auxquels nous faisons face dans le cyberespace. Alors que de plus en plus d'États développent des cybercapacités non seulement défensives, mais offensives aussi, il est essentiel que tous les États, dans leur utilisation des technologies numériques, se conforment au droit international existant et aux normes relatives au comportement responsable dans le cyberespace. Nous espérons que ces documents rappelleront aux États leurs obligations et contribueront ainsi à renforcer la stabilité dans le cyberespace.

Il va sans dire que les dispositions fondamentales de la Charte des Nations Unies devraient servir de guide à tous les États en ce qui concerne leur comportement dans le cyberespace. D'abord, les États sont tenus de se conformer à l'interdiction de l'emploi de la force, qui constitue le pilier central du régime international de sécurité. En outre, les précédents groupes d'experts gouvernementaux se sont entendus sur des normes de comportement responsable des États dans le cyberespace qui ont été approuvées par tous les États Membres. Il est donc clair que ce n'est pas l'absence de règles et de normes mais l'inapplication de celles-ci qui contribue à l'instabilité et à l'insécurité. Nous appelons donc tous les États à se conformer pleinement au droit international et à respecter l'ensemble des normes de comportement responsable des États.

Dans l'éventualité où un conflit armé ou des épisodes de celui-ci seraient déplacés dans le cyberespace, il est impératif que le droit international humanitaire soit respecté et appliqué : les principes d'humanité, de nécessité, de proportion, de distinction s'appliquent pleinement dans le cyberespace.

Dans le contexte de la pandémie de COVID-19, nous notons avec inquiétude la recrudescence récente des cyberattaques contre des hôpitaux et des établissements

sanitaires, une violation flagrante des normes selon lesquelles les infrastructures critiques, y compris les infrastructures médicales, ne devraient en aucun cas être visées par des cyberactivités malveillantes.

Afin d'éviter les scénarios de conflit, le renforcement de la confiance est essentiel ; les États devraient s'engager de manière constructive en partageant leur compréhension du cyberespace et leurs modes d'engagement militaire afin d'éviter les erreurs de jugement. À cet égard, le rôle des organisations régionales ne doit pas être sous-estimé : nombre d'entre elles ont mené des activités de renforcement de la confiance. Nous nous félicitons tout particulièrement de l'engagement de l'Organisation pour la sécurité et la coopération en Europe dans ce domaine et nous sommes convaincus qu'en nous appuyant sur son expérience d'un réseau de points de contact pour les questions de cybersécurité, nous pourrons également mettre en place un réseau mondial au niveau de l'ONU.

Si les États et les organisations internationales et régionales ont été à l'avant-garde de l'élaboration de lois et de normes internationales relatives au comportement responsable des États, ils ne peuvent relever tout seuls les défis auxquels nous faisons face. Les acteurs commerciaux ont un rôle important à jouer et une grande responsabilité à assumer dans le cyberespace, et la société civile et les milieux universitaires nous permettent d'avoir des points de vue différents dans nos débats. C'est pourquoi les prochains débats sur le cyberespace devraient être placés sous le signe d'une approche holistique et multipartite afin de faire en sorte que ceux qui ont un rôle à jouer dans les efforts visant à assurer un cyberespace libre, sûr, ouvert et stable soient entendus et contribuent aux objectifs que nous cherchons tous à atteindre.

Malgré tous les progrès réalisés dans le domaine de la cybersécurité, de nombreuses questions restent en suspens ; la communauté internationale devra apporter des réponses concertées à ces questions. La coopération restera essentielle et l'Autriche sera prête à participer de manière constructive aux initiatives pertinentes. Dans cet esprit, nous espérons que les futurs débats publics du Conseil se dérouleront selon les modalités d'avant, à savoir dans des conditions où les non-membres sont autorisés à faire des déclarations orales, le but étant de donner une visibilité à tous les États intéressés.

Annexe XX

Déclaration de M. Jamal Fares Alrowaiei, Représentant permanent de Bahreïn auprès de l'Organisation des Nations Unies

[Original : arabe]

La transformation technologique et numérique et l'émergence des technologies modernes contribuent au progrès, à la prospérité et au développement de l'humanité tout entière. L'importance de ces technologies a été amplifiée par le recours au travail, à l'enseignement et à la prestation de services à distance dans tous les secteurs durant la pandémie de maladie à coronavirus 2019 (COVID-19). Malgré les nombreux avantages du développement technologique, celui-ci comporte également de nombreux risques. C'est particulièrement le cas en l'absence d'un système de protection de la sécurité de l'information et du cyberespace clairement défini, comme le prouvent les nombreuses cyberattaques qui visent les infrastructures critiques des États et menacent des secteurs essentiels, des institutions ou des individus.

L'ONU a consacré une grande attention à cette question. Le Conseil de sécurité l'a abordée de manière indirecte lors de plusieurs réunions sur le maintien de la paix et de la sécurité internationales, ainsi que dans le cadre des réunions organisées selon la formule Arria. L'Assemblée générale a également créé un certain nombre de mécanismes, dont le Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Ce groupe a été créé en 2020 pour examiner les menaces posées par l'utilisation du numérique dans le contexte de la sécurité internationale, la formulation d'un code de comportement des États dans le cyberespace, l'application du droit international à l'utilisation des technologies numériques, les mesures de confiance et les activités de renforcement des capacités.

Fidèle à sa conviction qu'il est important de protéger le cyberespace contre les attaques et de garantir les intérêts des États et des peuples, Bahreïn a apporté son appui à la mise en place de ces mécanismes. Il a participé aux travaux du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui a achevé ses travaux en 2021. Bahreïn espère jouer un rôle actif au sein du groupe de travail nouvellement créé.

Au titre de l'intérêt particulier qu'il accorde à la cybersécurité au vu de la transformation numérique et du bond de géant des technologies numériques, Bahreïn s'est efforcé de mettre en place un système de gouvernance clair et complet pour protéger le cyberespace par l'intermédiaire du Centre national de cybersécurité du Ministère de l'intérieur, qui s'occupe de la cybersécurité dans divers secteurs du Royaume, et également par l'intermédiaire de l'Autorité de l'information et de l'administration numérique, qui protège la sécurité des informations dans le réseau de données du Gouvernement bahreïnien. L'autorité de réglementation des télécommunications s'efforce de renforcer la coopération entre les secteurs public et privé afin de se préparer à l'éventualité de menaces à la cybersécurité.

Bahreïn a également pris soin de mettre en place des cadres législatif et juridique pour assurer la sécurité de l'information, l'objectif étant de protéger les individus et les institutions. Parmi les lois adoptées à cet égard, on peut citer la loi n° 30 (2018) relative à la protection des données personnelles, la loi n° 16 (2014) relative à la protection de l'information et des documents étatiques et la loi n° 60 (2014) relative aux délits informatiques.

Au niveau régional, Bahreïn prend une part active aux travaux du Comité permanent sur la cybersécurité du Conseil de coopération des États arabes du Golfe (CCG). Il a proposé la création d'une plateforme électronique pour l'échange

d’informations et de données sur la cybersécurité entre les États membres. Chaque État membre a désigné un agent de liaison pour l’échange des informations sur la cybersécurité, notamment sur les menaces et les meilleures pratiques.

Le Royaume de Bahreïn a ratifié la Convention arabe sur la lutte contre les infractions liées aux technologies de l’information en 2017.

En conclusion, la délégation bahreïnienne affirme son attachement à la coopération internationale en matière de cybersécurité, en vue de répondre aux aspirations des peuples du monde et d’assurer le progrès, la prospérité et la croissance par la réalisation des objectifs de développement durable à l’horizon 2030.

Annexe XXI

Déclaration de M. Philippe Kridelka, Représentant permanent de la Belgique auprès de l'Organisation des Nations Unies

Je tiens tout d'abord à remercier la présidence estonienne d'avoir organisé ce premier débat public du Conseil de sécurité sur la paix et la sécurité dans le cyberespace. Ce débat opportun démontre l'urgente nécessité d'aborder ce sujet et l'importance que cela a pour le Conseil de sécurité. Les risques découlant d'activités malveillantes dans le cyberespace sont en effet de plus en plus élevés et leurs répercussions sur la paix et la sécurité internationales sont plus préjudiciables que jamais. Il est donc primordial de réaffirmer l'engagement des États Membres en faveur du droit international et du cadre de comportement responsable des États en tant qu'éléments clés de la prévention des conflits et du maintien de la paix et de la sécurité dans le cyberespace.

Pour atteindre cet objectif, il faut à la fois une vision internationale commune de la gouvernance du cyberespace et des mesures concrètes pour mettre en œuvre cette vision sur le terrain.

Le débat international sur la gouvernance du cyberespace est dans une étape décisive. La Belgique appuie vigoureusement les débats en cours au sein des entités de l'ONU, parmi lesquelles la Première Commission, les différents Groupes de travail à composition non limitée et Groupes d'éminents experts. Les éléments suivants sont essentiels :

Premièrement, la Belgique défend une vision commune d'un cyberespace mondial, libre, ouvert, stable, pacifique et sûr, où sont respectés les droits humains et les libertés fondamentales et dans lequel règne l'état de droit. Cette vision commune est fondée sur une approche globale qui permet à toutes les parties prenantes, y compris la société civile, le secteur privé et les milieux universitaires, de s'exprimer.

Deuxièmement, la communauté internationale doit continuer à s'efforcer de mettre en place un cadre de cybersécurité véritablement universel, pour un comportement responsable des États. Ce cadre doit se fonder sur le respect strict du droit international existant, y compris la Charte des Nations Unies dans son intégralité, du droit international humanitaire et du droit international des droits humains. L'année dernière, la Belgique, en tant que membre non-permanent du Conseil de sécurité, a participé à une réunion du Conseil organisée selon la formule Arria sur les cyberattaques contre les infrastructures critiques. Les cyberattaques visant les infrastructures critiques mettent des vies humaines en danger et doivent être condamnées par la communauté internationale. Les cyberattaques contre les établissements médicaux comme les hôpitaux sont inacceptables.

En ce qui concerne le cadre des Nations Unies de comportement responsable des États dans le cyberespace, il faut souligner que les États Membres de l'ONU ont approuvé, par l'adoption de la résolution 70/237 de l'Assemblée générale, les conclusions des rapports du Groupe d'experts gouvernementaux de 2010, de 2013 et de 2015, qui constituent une base solide et consensuelle pour des travaux supplémentaires. L'Organisation et ses États Membres ont déployé des efforts considérables pour parvenir à une vision internationale commune de la gouvernance du cyberespace et pour prendre des actions concrètes visant à mettre en œuvre cette vision commune sur le terrain. Dans un système multilatéral efficace et rationnel, il est impératif que nous fassions avancer tout nouveau débat en partant de cette base consensuelle, afin d'éviter de revenir sur les compromis laborieusement obtenus dans le passé tout en bloquant les efforts futurs.

Troisièmement, nous pensons que nous devrions mieux adapter la justice pénale internationale aux défis du XXIe siècle. C'est pourquoi la Belgique s'est associée au Liechtenstein dans son initiative de créer un Conseil consultatif sur l'application du Statut de Rome à la cyberguerre afin d'étudier le rôle que la Cour pénale internationale pourrait jouer dans ce nouveau cadre réglementaire. Nous attendons avec impatience le rapport final du Conseil consultatif, qui devrait être présenté cette année.

Les principes directeurs doivent être suivis d'actions pour donner des résultats. À cet égard, la Belgique est convaincue que le programme d'action proposé par l'Égypte et la France constitue la structure adéquate pour la mise en œuvre de notre vision. La Belgique est fière de soutenir cette initiative aux côtés de plus de 50 pays, et nous espérons que de nombreux autres États y adhéreront.

Au niveau national, la Belgique a récemment adopté, en mai 2021, une nouvelle stratégie nationale de cybersécurité 2.0 pour la période 2021-2025, dans laquelle notre pays décline son approche transversale en termes d'augmentation de sa cyberrésilience et de lutte contre les cybermenaces. L'objectif premier de cette stratégie nationale est « de faire de la Belgique l'un des pays les moins vulnérables d'Europe ».

Dans la politique de cybersécurité de la Belgique, il est également prévu de mettre au point un nouveau mécanisme d'attribution conçu comme un outil de dissuasion. Si nous voulons prévenir et dissuader efficacement les cyberactivités malveillantes dans un environnement où les cyberattaques sont de plus en plus nombreuses et complexes, l'attribution formelle d'une cyberactivité malveillante visant une organisation stratégique en Belgique est un instrument important. La procédure nationale d'attribution peut également être activée en vue de soutenir un pays allié victime d'attaques similaires.

En outre, on prescrit dans la stratégie nationale un engagement international clair. En effet, la Belgique joint le geste à la parole, convaincue qu'une coopération internationale accrue est nécessaire pour promouvoir la sécurité et la stabilité dans le cyberespace.

Une coopération internationale accrue signifie également un renforcement des capacités et de l'attachement aux mesures de confiance, notamment grâce aux efforts d'organisations régionales telles que l'Organisation pour la sécurité et la coopération en Europe (OSCE). La Belgique prend une part active aux travaux de l'OSCE pour rendre ces mesures de confiance concrètes et opérationnelles. Quant au renforcement des capacités, les besoins sont considérables et urgents au niveau mondial. Les programmes de coopération ou de renforcement des capacités existants, tels que ceux proposés par l'Union européenne ou par le Forum mondial sur la cyberexpertise, doivent être renforcés et étendus. Il est dans notre intérêt à tous de renforcer la résilience mondiale face aux cybermenaces.

Annexe XXII

Déclaration de la Mission permanente du Brésil auprès de l'Organisation des Nations Unies

Tout d'abord, je tiens à féliciter l'Estonie pour la grande initiative consistant à promouvoir, pour la première fois, un débat public officiel du Conseil de sécurité sur la cybersécurité dans le contexte plus large du maintien de la paix et de la sécurité internationales. L'évolution rapide des technologies numériques, qui ont fini par s'introduire dans tous les domaines de la vie humaine, nous oblige à actualiser le concept de menaces, à adapter le cadre normatif existant à cette nouvelle réalité et à élaborer de nouveaux modèles de comportement responsable des États afin de relever les défis modernes et de freiner l'émergence de conflits.

Bien que le thème de la cybersécurité vienne tout juste d'être abordé au sein de l'organe auquel incombe la responsabilité principale du maintien de la paix et de la sécurité internationales, les États Membres en débattent depuis plus d'une vingtaine d'années – au moins depuis 1998, date à laquelle le sujet a été inscrit pour la première fois à l'ordre du jour de l'Assemblée générale. Au cours de cette période, nous avons assisté à l'adoption de quatre rapports consensus de groupes d'experts gouvernementaux, dont deux présidés par des experts brésiliens, et d'un autre rapport de consensus d'un groupe de travail à composition non limitée. Collectivement, ces documents forment un *acquis communautaire*, c'est-à-dire un ensemble commun d'ententes et de normes, règles et principes volontaires non contraignants qui permettent de régir l'utilisation des technologies numériques par les États.

L'une des plus grandes contributions de cet *acquis communautaire* au maintien de la paix et de la sécurité internationales, c'est la confirmation que le droit international, y compris le droit international humanitaire, est applicable au cyberespace. Dans notre contribution nationale volontaire au recueil officiel du dernier Groupe d'experts gouvernementaux, nous avons réaffirmé la ferme conviction du Brésil que, dans leur utilisation des technologies numériques, les États doivent respecter le droit international, y compris la Charte des Nations Unies, le droit international des droits humains et le droit international humanitaire. L'ONU et d'autres organisations régionales ont reconnu que le droit international, et en particulier la Charte des Nations Unies, est applicable au cyberespace et essentiel au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement ouvert, sûr, pacifique et accessible en matière d'informatique et de technologies des communications. Ainsi, dans les débats actuels, la question n'est plus de savoir si le droit international s'applique à l'utilisation des technologies numériques par les États, mais la manière dont elle s'y applique.

Si les analogies avec le monde physique peuvent fonctionner la plupart du temps pour déterminer cette application, les caractéristiques atypiques du cyberespace créent de nouvelles situations dont la réglementation n'était pas prévue par le droit international à la base. L'interconnectivité des systèmes d'information, le caractère immatériel de l'environnement numérique et la complexité du problème de l'attribution de la responsabilité des actes malveillants et offensants dans le cyberespace, entre autres facteurs, posent de nouveaux défis au droit international établi sur la base d'un ordre international physique et territorial.

Les différences d'interprétation par les États de l'application du droit international à l'utilisation des technologies numériques augmentent le risque de comportements imprévisibles, de malentendus et d'escalade des tensions. Il importe donc de recenser progressivement les domaines de convergence entre les États en la matière et, lorsqu'il existe des divergences, d'œuvrer conjointement à harmoniser davantage l'interprétation des règles existantes. Si nécessaire, ils devraient également

envisager d'élaborer des normes supplémentaires en vue de combler les éventuels vides juridiques et de résoudre les incertitudes qui persistent.

Le maintien de la paix et de la sécurité internationales dépend fortement du niveau de confiance qui existe entre les États. Par conséquent, outre la reconnaissance de l'applicabilité du droit international et la création et l'application de normes, de règles et de principes de comportement responsable des États, il est primordial que les États mettent en place des mesures de confiance. La mise en place d'un réseau de points de contact aux niveaux technique et politique, ainsi que l'échange de points de vue nationaux sur les menaces et sur la gestion des actes de cybermalveillance sont des mesures importantes de coopération et de transparence. Ces initiatives permettent non seulement de prévenir les malentendus et les erreurs de jugement, mais sont également utiles pour la gestion des événements graves liés au numérique et le désamorçage des tensions en cas de crise.

Le renforcement des capacités est également un outil essentiel à la promotion d'un environnement numérique pacifique. Comme dans d'autres domaines, l'inégalité entre les nations peut également être à l'origine de l'insécurité dans le cyberespace, avec des effets directs sur le monde cinétique. La coopération internationale pour le développement des institutions nationales, le renforcement des capacités des ressources humaines et l'élaboration de politiques publiques contribue à réduire les vulnérabilités des États et est fondamentale pour l'universalisation de l'application du droit international et des normes, règles et principes de comportement responsable des États dans le cyberespace. S'il y a un enseignement à tirer de la pandémie, c'est que personne n'est à l'abri tant que tout le monde ne l'est pas ; le même raisonnement peut être appliqué au cyberespace, hautement interconnecté et interdépendant.

Compte tenu de la nature multipartite du cyberespace, le Brésil estime qu'aucun vrai débat sur la cybersécurité ne peut aboutir sans la contribution de la société civile, des milieux universitaires et du secteur privé. Il est essentiel d'adopter une approche multipartite en vue d'identifier et d'écarter les menaces, de prévenir les conflits, de promouvoir des visions communes, d'accroître la cyberrésilience et de favoriser la coopération. Une interaction plus large entre les acteurs publics et privés de différents pays, la mise en commun de données d'expériences et l'échange des meilleures pratiques sont essentiels pour parvenir à un environnement numérique plus ouvert, plus sûr, plus pacifique et plus accessible.

Le Brésil a pris une part active aux débats sur la cybersécurité dans le cadre de l'Organisation des Nations Unies. Nous avons toujours cherché à adopter une approche anticipative, au sein des groupes d'experts gouvernementaux comme au sein du nouveau Groupe de travail à composition non limitée. Le Brésil continuera de jouer un rôle actif dans les débats du nouveau Groupe de travail à composition non limitée, qui tiendra sa première session de fond en décembre, ainsi que dans les autres mécanismes de dialogue institutionnel régulier qui pourraient être mis en place, tels que le programme d'action sur la cybersécurité. En même temps, en tant que membre non permanent nouvellement élu du Conseil de sécurité, notre pays a l'intention de contribuer également à faire avancer au sein de cet organe les débats sur les effets de l'utilisation des technologies numériques dans le contexte de la sécurité internationale. Selon le Brésil, le Conseil devrait être guidé avant tout par l'objectif de promouvoir l'application des recommandations formulées par l'Assemblée générale dans le passé sur la question de la cybersécurité et celles qu'elle formulera à l'avenir.

Annexe XXIII

Déclaration de la Mission permanente du Canada auprès de l'Organisation des Nations Unies

[Original : français]

Nous remercions l'Estonie d'avoir organisé cette séance du Conseil de sécurité sur un sujet aussi opportun et pertinent. Le Canada est heureux d'avoir l'occasion de contribuer à cette discussion.

Le monde dépend de plus en plus des technologies numériques et de l'Internet. Le cyberespace pose de nombreuses menaces à la paix et la sécurité internationales. L'ingérence dans la vie démocratique est un domaine particulièrement préoccupant. L'augmentation récente des attaques aux logiciels rançonneurs en est un autre. Nous devons donc continuer à prendre des mesures pour que le cyberespace demeure libre, ouvert et sécuritaire.

Le cadre convenu pour favoriser le comportement responsable des États dans le cyberespace est le fondement sur lequel reposent la paix et la stabilité dans cet espace. Ce cadre consiste à reconnaître l'applicabilité du droit international au cyberespace, à adhérer aux normes convenues à l'échelle internationale, à renforcer les capacités, ainsi qu'à mettre en œuvre des mesures de renforcement de la confiance. Ensemble, ces éléments réduisent les risques d'escalade et de conflit.

Ce cadre a été réaffirmé dans les rapports consensuels récemment adoptés par le Groupe de travail à composition non limitée et le Groupe d'experts gouvernementaux des Nations Unies. Tous les États Membres des Nations Unies se sont désormais engagés à être guidés par ce cadre.

Le droit international est essentiel à l'application au cyberespace de l'ordre international fondé sur des règles. Les rapports publiés récemment par le Groupe de travail et le Groupe d'experts gouvernementaux réaffirment l'applicabilité du droit international au cyberespace et font des avancées importantes à cet égard. Le rapport du Groupe de travail recommande une plus grande coopération dans le renforcement des capacités en droit international, afin qu'un plus grand nombre d'États puissent formuler leur propre conception et bâtir un point de vue commun. Dans le rapport du Groupe d'experts gouvernementaux, l'applicabilité du droit international a été réaffirmée et le droit international humanitaire a été expressément mentionné.

Le rapport produit par le Groupe d'experts gouvernementaux en mai 2021 guide la mise en œuvre des 11 normes non contraignantes de comportement responsable des États. Ces normes ont été adoptées par le Groupe d'experts gouvernementaux des Nations Unies en 2015 et approuvées par tous les États Membres dans la résolution 70/237 de l'Assemblée générale. Le Canada estime que ces normes et le droit international sont largement suffisants pour guider le comportement des États dans le cyberespace. Toutefois, il reste du travail à faire dans leur diffusion et leur application.

Prenons les récentes attaques aux logiciels rançonneurs très médiatisées, perpétrées par des groupes criminels. Elles ont perturbé à grande échelle des secteurs clefs tels que l'énergie et l'approvisionnement alimentaire. Elles ont aussi affecté les marchés financiers.

Bien que des groupes criminels soient responsables de ces actes, ces exemples soulignent l'importance du droit international et des 11 normes du Groupe d'experts gouvernementaux. Plusieurs de ces normes traitent directement ou indirectement des menaces que les TIC font peser sur les infrastructures essentielles. Une des normes stipule que les États doivent répondre aux demandes d'assistance formulées par tout

État dont l'infrastructure essentielle fait l'objet d'actes malveillants au moyen des TIC. Une autre stipule que les États ne doivent pas permettre sciemment que leur territoire serve à la perpétration d'actes illicites à l'échelle internationale au moyen des TIC.

Les groupes qui se livrent à des actes criminels, dont les attaques aux logiciels rançonneurs, vivent et travaillent dans des États. Ils se servent de l'infrastructure numérique de ces États pour se livrer à ces actes, alors qu'ils sont assujettis à leurs lois. Les États qui apprennent qu'un acte malveillant émane de leur territoire ont la responsabilité d'agir, de faire appliquer leurs lois et de coopérer avec les autres États. En acceptant d'être guidés par les normes du Groupe d'experts gouvernementaux, nous nous sommes tous engagés à agir ainsi. C'est aussi la raison pour laquelle un nombre croissant d'États ont adopté des lois strictes dans la lutte contre la cybercriminalité. Dans de nombreux cas, ces États ont fondé ces lois sur la Convention sur la cybercriminalité du Conseil de l'Europe, également connue sous le nom de Convention de Budapest, qui compte désormais des parties de toutes les régions du monde.

Malheureusement, comme nous l'avons récemment constaté, les États ne respectent pas tous et pas toujours le cadre sur le comportement responsable des États. Certains pays permettent aux cybercriminels d'opérer depuis leur territoire en toute impunité. D'autres passent par des intermédiaires ou se livrent délibérément à des cyberactivités malveillantes qui vont à l'encontre du cadre. À plusieurs reprises, le Canada s'est joint à ses partenaires internationaux pour dénoncer ces comportements et réagir à la menace qu'ils représentent pour la paix et la sécurité internationales.

Le Canada est l'un des 27 signataires de la déclaration commune de septembre 2019 sur la promotion d'un comportement responsable par les États dans le cyberespace. En plus de réaffirmer le cadre convenu pour favoriser un comportement responsable de la part des États dans le cyberespace, nous nous sommes engagés à « travailler ensemble et de plein gré à tenir les États responsables lorsqu'ils agissent contrairement à ce cadre, notamment en prenant des mesures transparentes et conformes au droit international ».

C'est ce que nous avons fait jusqu'à présent, et c'est ce que nous continuerons de faire. Il est important de révéler au grand jour les comportements contre-normatifs, afin de faire respecter le cadre convenu pour favoriser un comportement responsable de la part des États dans le cyberespace. Nous encourageons tout le monde à faire de même.

Pour ce qui est de l'avenir à l'Organisation des Nations Unies (ONU), le Canada se réjouit de participer de manière constructive au Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Nous contribuerons aussi à l'élaboration d'un programme d'action des Nations Unies sur la cybersécurité. Le Canada est coauteur de ce programme d'action, car nous estimons que ce programme peut servir de forum utile et axé sur l'action qui favorisera la mise en œuvre du cadre pour le comportement responsable des États.

La réussite de ces deux processus dépendra de leur capacité à intégrer des voix et des perspectives diverses dans leurs méthodes de travail et leurs résultats. Au sein du Groupe de travail à composition non limitée, le Canada plaide en faveur d'une participation significative des parties prenantes non gouvernementales. En effet, la société civile, le milieu universitaire, le monde technique et le secteur privé ont beaucoup à apporter à ces discussions, car ils jouent un rôle important dans la mise en œuvre des recommandations du Groupe d'experts gouvernementaux et du Groupe de travail. Nous plaiderons également en faveur d'un engagement fort des parties prenantes dans le programme d'action, au fur et à mesure de son élaboration.

Il sera également important de veiller à ce que les voix des femmes soient réellement entendues, que ce soit au sein du Groupe de travail à composition non limitée ou de l'élaboration du programme d'action. Le genre doit être intégré dans les deux processus dès le départ, afin que les aspects de la cybersécurité liés au genre soient abordés dans les travaux des deux groupes. Il est bien documenté que les médiations où la participation féminine est importante aboutissent à une paix beaucoup plus solide, caractérisée par un risque moindre de reprise des hostilités. Les cyberprocessus de l'ONU peuvent être renforcés de la même manière, en y faisant participer les femmes de manière importante. L'inclusion est importante pour la réussite des deux processus.

En bref, le Canada demeure un partisan indéfectible du cadre convenu pour favoriser un comportement responsable de la part des États dans le cyberespace. Nous continuerons à promouvoir la mise en œuvre des recommandations des Groupes d'experts gouvernementaux précédents et du récent Groupe de travail à composition non limitée. Nous continuerons également à dénoncer et à répondre aux cyberactivités malveillantes qui vont à l'encontre de ce cadre. Nous nous réjouissons de continuer à travailler avec la communauté internationale dans la promotion de la paix et de la sécurité internationales en renforçant la stabilité et la sécurité dans le cyberespace.

Annexe XXIV

Déclaration de la Mission permanente du Chili auprès de l'Organisation des Nations Unies

Le Chili réaffirme sa position selon laquelle le droit international, et 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. Ce principe, ainsi que les principes correspondants de la Charte des Nations Unies, en particulier le règlement pacifique des différends, l'interdiction de recourir à la menace ou à l'emploi de la force contre l'intégrité territoriale ou l'indépendance politique d'un État, le principe de non-intervention dans les affaires intérieures d'autres États et le respect des droits humains et des libertés fondamentales, sont indissociables dans le domaine physique comme dans le domaine numérique et, à ce titre, le Chili continuera à promouvoir son application.

Les activités malveillantes menées dans le cyberespace par les mêmes acteurs, parmi lesquels se trouvent des États et d'autres parties prenantes, peuvent créer un risque considérable pour la sécurité et la stabilité internationales, pour le développement économique et social ainsi que pour la sécurité et le bien-être des personnes. Les activités malveillantes contre les infrastructures critiques qui fournissent des services au niveau national, régional ou mondial sont de plus en plus graves, notamment les activités malveillantes menées dans le cyberespace qui touchent les infrastructures d'information critiques, les infrastructures fournissant des services essentiels au public, les infrastructures techniques essentielles à la disponibilité générale ou à l'intégrité d'Internet et les entités du secteur de la santé. Dans les conflits futurs, ces activités malveillantes peuvent être plus destructrices et compromettre sérieusement le bien-être et la vie des populations. En ce sens, les pays pourraient être sérieusement touchés par des cyberattaques lancées dans le cadre de conflits armés.

Pendant les conflits armés, les États devraient planifier, conduire et exécuter leurs opérations dans le cyberespace en respectant strictement les règles du droit international, en accordant une attention particulière au droit international des droits humains et au droit international humanitaire.

Le Chili soutient fermement les travaux du Groupe d'experts gouvernementaux, trouve utiles ses rapports et s'associe à ses recommandations formulées en 2010, en 2013, en 2015 et en 2021, car ils ont constitué une énorme avancée en matière de droit international, de normes et de mesures de confiance dans le domaine du numérique. Le Chili soutient également les travaux du Groupe de travail à composition non limitée et fait siennes ses recommandations. Pour réduire l'utilisation malveillante des cybercapacités et stabiliser davantage le cyberespace, il importe de suivre et d'appliquer ces recommandations à tous les niveaux.

Le programme d'action pour la promotion d'un comportement responsable des États dans le cyberespace est une initiative positive, constructive et réaliste qui pourrait nous aider à progresser et à obtenir des résultats concrets dans le cadre de l'environnement numérique. Il pourrait être un instrument international permanent, inclusif, consensuel et pragmatique destiné à promouvoir un comportement responsable dans l'utilisation des technologies numériques dans le contexte de la sécurité internationale. En tant que coparrain de cette initiative, le Chili estime que le programme d'action offrirait une plateforme pour formuler des recommandations opérationnelles, promouvoir la coopération internationale et favoriser des programmes d'assistance adaptés aux besoins des États bénéficiaires, notamment en matière de renforcement des capacités.

En ce qui concerne le respect du droit international existant et la mise en œuvre des normes de comportement responsable des États dans le cyberespace, il importe que les États puissent développer et partager leurs points de vue avec d'autres États sur la manière dont le droit international s'applique dans le cyberespace. Le renforcement des capacités dans ce domaine est également crucial. L'adoption de principes directeurs pour la mise en œuvre des normes est une mesure importante qui devrait aider les États à faire des progrès en la matière. Les organisations régionales peuvent jouer un rôle clé en aidant les États à mettre en œuvre les normes et à respecter le droit international, en élaborant des stratégies régionales à cet égard, ainsi qu'en assurant la formation et le renforcement des capacités.

Le Chili estime qu'il est fondamental de renforcer les mesures de confiance dans le cyberespace et de rendre plus efficace le renforcement des capacités, les organisations régionales devant y jouer un rôle primordial. À cet égard, nous soulignons le travail effectué par l'Organisation des États américains par l'intermédiaire de son groupe de travail sur la coopération et les mesures de confiance dans le cyberespace, ainsi que le travail et les progrès réalisés par l'Organisation pour la sécurité et la coopération en Europe et l'Association des nations de l'Asie du Sud-Est.

Il importe de promouvoir le dialogue entre les régions à ce sujet, mais aussi en matière de renforcement des capacités et de mise en œuvre des normes. Dans le cadre de ce dialogue, on devrait envisager l'échange de données d'expériences, d'informations, de principes directeurs, de meilleures pratiques et d'enseignements, et inviter les membres des organisations à participer à ces mécanismes régionaux. Les États devraient renforcer leurs points de contact nationaux, ainsi que le rôle de leurs ministères des affaires étrangères en ce qui concerne les politiques relatives au cyberespace et aux technologies numériques. La cyberdiplomatie est un outil important qui peut aider les États à améliorer leur coopération et à renforcer la confiance. Les États devraient également envisager d'établir des mécanismes bilatéraux de dialogue et de coopération sur la cybersécurité et le cyberespace.

Le Chili estime que les mécanismes multilatéraux doivent être aussi inclusifs et transparents que possible. On devrait faire une place au secteur privé, aux milieux universitaires, à la société civile, à l'industrie et aux spécialistes techniques, entre autres, dans le débat sur le numérique. Il n'est pas possible de créer un environnement stable et sûr dans le cyberespace si nous ne garantissons pas la participation et le travail de toutes les parties prenantes. Plus le nombre de participants au débat est élevé, plus nous avons de chances d'obtenir des résultats bénéfiques pour tous. En ce sens, nous pensons qu'il est nécessaire que nous puissions écouter toutes les parties intéressées et que celles-ci puissent également présenter leurs points de vue et apporter leurs contributions lors des sessions officielles. À cet égard, les États devraient faire participer toutes les parties prenantes lorsqu'il s'agit d'élaborer des politiques, des stratégies et d'autres initiatives visant à prévenir les conflits, à établir une vision commune et à renforcer la cyberrésilience.

Annexe XXV

Déclaration de la Mission permanente de la République tchèque auprès de l'Organisation des Nations Unies

La République tchèque tient à remercier la République d'Estonie d'avoir organisé le tout premier débat public du Conseil de sécurité sur le thème de la cybersécurité dans le contexte de la paix et de la sécurité internationales. Le respect du droit international par les États et le fait qu'ils se comportent de manière responsable dans le cyberespace sont des éléments clés de la prévention des conflits et du maintien de la paix et de la sécurité internationales.

La République tchèque s'associe à la déclaration de l'Union européenne et tient à insister sur les deux points supplémentaires ci-après.

Cybermenaces actuelles et nouvelles pesant sur la paix et la sécurité internationales

Le cyberespace offre des avantages considérables pour le développement humain et économique, mais il devient également un domaine où les dépendances et les problèmes de sécurité sont de plus en plus nombreux. Notre dépendance accrue aux technologies pendant la pandémie de maladie à coronavirus 2019 (COVID-19), qui est continuellement exploitée par des acteurs malveillants pour leur propre intérêt, nous rappelle clairement le nombre de plus en plus élevé de défis à relever dans le cyberespace. Nous avons notamment constaté une augmentation alarmante des cyberactivités malveillantes dirigées contre des infrastructures critiques fournissant des services essentiels au public, notamment celles visant les établissements médicaux, les infrastructures d'eau, d'électricité, d'assainissement, les infrastructures électorales et la disponibilité générale d'Internet. En particulier, le nombre croissant de cyberattaques qui perturbent la fourniture de soins de santé entraîne de nouvelles pertes de vies humaines, compromet notre capacité collective à lutter contre la COVID-19 et, en définitive, menace la paix et la stabilité internationales.

De telles cyberactivités irresponsables visant à endommager intentionnellement des infrastructures critiques risquent également d'avoir des conséquences humanitaires potentiellement dévastatrices et, si elles sont imputables à un État, elles constitueraient un manquement aux obligations des États en vertu du droit international. La République tchèque se félicite donc du fait que tous les États Membres ont récemment affirmé, dans les rapports finaux du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée, que les cyberactivités dirigées contre les infrastructures critiques sont inacceptables. Si un engagement politique est la première étape nécessaire, la protection des infrastructures critiques contre les cybermenaces nécessitera également des efforts concrets et durables de la part de la communauté internationale, notamment par le renforcement de la coopération technique et des programmes pratiques de renforcement des capacités dans le domaine des technologies numériques. Le Conseil de sécurité peut également jouer un rôle décisif en veillant à ce que les cyberactivités parrainées par des États et dirigées contre des infrastructures critiques soient sanctionnées.

Les cybermenaces actuelles et nouvelles compromettent non seulement la sécurité interne des États, mais menacent aussi de plus en plus le bien-être et la sécurité des individus. La République tchèque est particulièrement préoccupée par le clivage politique croissant entre les États qui prônent la protection des libertés individuelles dans le cyberespace et ceux qui appellent à une surveillance technologique accrue. Selon nous, la multiplication des techniques de surveillance de masse par les pouvoirs publics au moyen des technologies numériques, les blocages

partiels ou complets d'Internet et la censure généralisée des contenus soulèvent de graves préoccupations en matière de droits humains. Il est essentiel d'entreprendre une action ferme pour la protection des citoyens contre l'exercice arbitraire et illégal du pouvoir de l'État dans le cyberespace. Ces tendances, conjuguées aux risques potentiels liés à l'introduction de l'intelligence artificielle dans diverses facettes de notre vie, posent de nouveaux défis en matière de sécurité, menacent d'ébranler la confiance dans le cyberespace et peuvent, à terme, dégrader notre capacité à maintenir la paix et la sécurité internationales.

Respecter davantage le droit international et les normes de comportement responsable des États

La République tchèque tient à rappeler que le respect par les États des obligations qui leur incombent en vertu du droit international est un élément essentiel au maintien d'un cyberespace libre, pacifique, stable, sûr, interopérable et accessible. Tous les États ont affirmé le bien-fondé de l'application du droit international existant à l'utilisation des technologies numériques par les États, notamment par l'approbation universelle des rapports du groupe d'experts gouvernementaux de 2013 et de 2015 dans les résolutions 68/243 et 70/237 de l'Assemblée générale.

À cet égard, la République tchèque rappelle également que le droit des États d'exercer une juridiction exclusive sur les technologies numériques se trouvant sur leur territoire donne lieu non seulement à des droits mais aussi à des obligations particulières en vertu du droit international. En particulier, la République tchèque souhaite réaffirmer que les corpus juridiques existants, notamment le droit international humanitaire et le droit international des droits humains, s'appliquent au comportement des États dans le cyberespace sans exception.

Malheureusement, une petite minorité d'États continue de remettre en question le bien-fondé de l'application du droit international existant au cyberespace, notamment l'application du droit international humanitaire à l'utilisation des technologies numériques dans le contexte des conflits armés. La République tchèque tient à souligner qu'elle est d'avis que la possibilité d'appliquer le droit international humanitaire aux cyberactivités ne favorise pas la militarisation du cyberespace, pas plus qu'elle ne favorise la militarisation de quelque autre domaine que ce soit. Au contraire, le droit international humanitaire impose des limites à l'emploi de la force en exigeant que toute utilisation de moyens et de méthodes de combat dans le cadre d'un conflit armé soit conforme à ses principes, notamment les principes d'humanité, de distinction et de proportionnalité.

En outre, la République tchèque rappelle que, conformément au droit de la responsabilité pour fait internationalement illicite, tous les États ont l'obligation d'observer les précautions qui s'imposent et de prendre des mesures concrètes, dans la mesure de leurs moyens, pour veiller à ce que leur territoire ne soit pas utilisé pour mener des cyberactivités malveillantes contre d'autres États.

La République tchèque reconnaît également que la capacité d'un État à mettre en œuvre le cadre existant de comportement responsable des États dans le cyberespace, y compris sa capacité à observer de manière adéquate les précautions qui s'imposent, est intrinsèquement liée aux capacités de cet État. À cet égard, la République tchèque souligne la nécessité d'intensifier les efforts internationaux visant à renforcer la cybercapacité et accroître la cyberrésilience à l'échelle mondiale, notamment par la mise en place rapide du programme d'action des Nations Unies pour un comportement responsable des États dans le cyberespace, qui permettrait aux États Membres de faire progresser l'exécution des engagements déjà pris par une action concrète et axée sur les résultats.

En conclusion, la République tchèque est pleinement attachée à une approche de la cybersécurité centrée sur l'être humain, qui met l'accent sur la nécessité de protéger la sûreté et la sécurité des personnes dans l'environnement numérique, que ce soit en protégeant les infrastructures critiques contre les cybermenaces ou en veillant à ce que les mesures de cybersécurité ne servent pas de prétexte pour restreindre le plein exercice des droits humains et des libertés fondamentales dans le cyberespace.

Annexe XXVI

Déclaration conjointe des missions permanentes du Danemark, de la Finlande, de l'Islande, de la Norvège et de la Suède auprès de l'Organisation des Nations Unies

J'ai le plaisir de prendre la parole au nom des pays nordiques : la Finlande, l'Islande, la Norvège, la Suède et mon pays, le Danemark. Nous remercions la présidence estonienne d'avoir inscrit cette question très pertinente à l'ordre du jour du Conseil. C'est une excellente occasion pour tous les États Membres d'aller au-delà de notre engagement en faveur de l'application du droit international dans le cyberespace et du cadre d'un comportement responsable des États dans le cyberespace, le but étant de promouvoir la paix et la stabilité.

Le monde tire de multiples avantages du développement des technologies numériques. Ces technologies sont à l'origine d'un progrès économique et d'un développement sociétal considérables. Dans le contexte de la pandémie actuelle, le cyberespace a permis à nombre d'entre nous de rester en contact avec notre famille, nos amis et nos collègues, et de maintenir des fonctions importantes de la société, notamment le fonctionnement d'infrastructures critiques qui sont essentielles à la gestion de la crise sanitaire. Néanmoins, le cyberespace a également été utilisé pour diffuser de fausses informations sur le virus responsable de la COVID-19, exposant ainsi notre vulnérabilité collective aux perturbations et au mauvais usage du cyberespace. De plus, la pandémie a mis au jour de profondes fractures numériques, particulièrement celle entre les genres. En tant que pays nordiques, nous sommes fermement convaincus qu'un cyberespace accessible, libre, ouvert et sûr à l'échelle mondiale est fondamental non seulement pour le fonctionnement du monde actuel, mais aussi pour notre ambition commune de construire un avenir meilleur, plus vert et plus sûr.

Malheureusement, les cyberactivités malveillantes continuent de menacer la sécurité et la stabilité du cyberespace. Ces dix-huit derniers mois ont révélé que les acteurs étatiques et non étatiques saisiront toute occasion, même une pandémie, pour mener des activités malveillantes dans le cyberespace. De telles activités sont inacceptables. Elles menacent l'intégrité, la sécurité et la prospérité de nos sociétés et fragilisent la paix et la stabilité internationales.

Permettez-moi de souligner trois tendances interdépendantes qui constituent un obstacle à la paix et à la sécurité internationales.

Premièrement, la récente augmentation des cyberattaques contre les chaînes d'approvisionnement des entreprises, des organisations et des administrations publiques a rendu des dizaines, voire des centaines de milliers de systèmes informatiques vulnérables. Ces attaques révèlent un mépris flagrant pour les acteurs concernés. L'objectif est souvent de voler des informations sensibles et de la propriété intellectuelle pour obtenir un avantage dans la concurrence géopolitique. De telles attaques peuvent avoir d'autres effets imprévus, car les portes dérobées sont laissées ouvertes et n'importe qui peut les exploiter.

Deuxièmement, des cyberattaques perturbatrices parrainées par des États, telles que WannaCry et NotPetya, ont été lancées dans le monde en faisant totalement fi des effets systémiques négatifs qu'elles peuvent avoir à l'échelle mondiale. Ces attaques n'ont pas seulement entraîné d'importantes pertes financières, elles ont également paralysé les systèmes informatiques, notamment dans les hôpitaux, ainsi que les systèmes de contrôle industriels, ce qui a eu des effets sur l'approvisionnement crucial en électricité. Ces activités compromettent la santé et la sécurité de nos citoyens.

Troisièmement, les États doivent prendre des mesures contre les effets de plus en plus graves et déstabilisants de la cybercriminalité émanant de leur territoire. Les récentes attaques par logiciel rançonneur contre l'approvisionnement en carburant aux États-Unis, contre les hôpitaux en Irlande et contre la production alimentaire au Brésil, aux États-Unis et en Australie montrent que les conséquences de la cybercriminalité sont devenues une préoccupation de sécurité nationale avec des effets possibles sur la paix et la sécurité internationales. La fusion de plus en plus fréquente entre acteurs étatiques et acteurs non étatiques rend la menace encore plus complexe.

De jour en jour, le seuil du comportement toléré dans le cyberespace évolue dans la mauvaise direction. Nous devons inverser cette tendance en respectant l'engagement commun que nous, les États Membres, avons pris lorsque nous avons approuvé les rapports du Groupe d'experts gouvernementaux et le rapport de consensus du Groupe de travail à composition non limitée. Dans cet esprit, nous réaffirmons que le droit international, y compris la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international des droits humains, s'applique au comportement des États dans le cyberespace. Nous appelons également à un plus grand respect des 11 normes facultatives et non contraignantes de comportement responsable des États dans le cyberespace, définies dans le rapport du Groupe d'experts gouvernementaux de 2015, sans perdre de vue les orientations et le nouveau niveau d'interprétation de ces normes qu'on trouve dans le rapport du Groupe d'experts gouvernementaux de 2021. Cela contribuerait grandement à relever les défis mentionnés plus haut.

Nous devons alourdir les sanctions punissant la cyberactivité malveillante en faisant collectivement en sorte que les responsables répondent de leurs actes. Tous les États doivent faire preuve de la diligence requise et prendre les mesures appropriées pour lutter contre la cyberactivité malveillante émanant de leur territoire. Les groupes de hackers ne doivent pas être autorisés à agir en toute impunité.

Nous sommes favorables à la poursuite de l'échange d'informations et de bonnes pratiques au sein de l'ONU, notamment en ce qui concerne l'application des normes de comportement responsable des États, les mesures de confiance et l'application du droit international existant dans le cyberespace. Nous devrions chercher à adopter une approche orientée vers l'action, qui s'appuie sur le cadre consensuel que nous avons déjà accepté avec l'approbation par l'Assemblée générale du rapport du Groupe de travail à composition non limitée et des rapports du Groupe d'experts gouvernementaux. Cette approche constituera l'élément de base de toute discussion à l'avenir. Le programme d'action proposé est un bon moyen d'avancer vers l'application intégrale des normes déjà acceptées.

Nous devons reconnaître que si la cybermenace est un problème mondial, elle se manifeste différemment selon les pays et les régions. La promotion d'une cyberrésilience solide dans toutes nos sociétés est crucial non seulement pour notre sécurité commune, mais aussi pour l'exercice des droits humains. Nous devons coopérer pour renforcer les capacités au niveau mondial.

Les États ne peuvent pas y arriver seuls. La lutte contre les menaces dans le cyberespace nécessite une approche multipartite permettant de prévenir les conflits, d'établir une vision commune et de renforcer la confiance et les capacités. Nous avons besoin que l'ONU soit une instance rassembleuse et une plateforme pour établir une coopération efficace entre les gouvernements, la société civile, les milieux universitaires et le secteur privé. Nous sommes en faveur du Plan d'action de coopération numérique, en particulier pour ce qui est de la participation du secteur privé, ce qui est essentiel pour la gestion des infrastructures critiques, la collecte des informations et la protection des systèmes et des données personnelles.

Tous les États doivent assumer leur responsabilité et se conformer au droit international et respecter les normes dans le cyberespace. S'ils ne le font pas, la menace que la cyberactivité malveillante fait peser sur la paix et la sécurité internationales continuera de croître. Les cyberattaques continueront d'accroître le risque de conflit, de mettre en danger des vies humaines, de violer les droits humains, d'étouffer l'activité économique, d'approfondir les divisions et de provoquer des différends. Tous les États ont un rôle à jouer dans la promotion et le maintien d'un cyberespace fondé sur des règles, prévisible, ouvert, équitable, libre, accessible, stable et sûr, dans l'intérêt de tous.

Annexe XXVII

Déclaration de M. Cristian Espinosa, Représentant permanent de l'Équateur auprès de l'Organisation des Nations Unies

[Original : espagnol]

Permettez-moi tout d'abord de féliciter l'Estonie d'avoir inscrit cette question à l'ordre du jour du Conseil de sécurité un an après la réunion organisée selon la formule Arria sur le sujet. Je tiens également à rappeler le rôle prépondérant de la Première Ministre Kaja Kallas sur cette question.

Je voudrais également souligner la présentation de M^me^ Izumi Nakamitsu, Secrétaire générale adjointe et Haute-Représentante pour les affaires de désarmement.

Cet exercice 2020-2021 a marqué une étape importante dans la cyberdiplomatie, non seulement en raison du mandat et des résultats obtenus sur les questions de fond le 12 mars 2021 par le premier Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et du consensus obtenu le 28 mai 2021 par le Groupe d'experts gouvernementaux sur le comportement responsable des États dans le cyberespace, mais aussi en raison de la crise de la pandémie de COVID-19 qui a accéléré la transformation numérique.

La pandémie a eu des répercussions différentes sur toutes les dimensions de la paix et de la sécurité. La cybersécurité n'a pas fait exception. La sécurité des services essentiels est devenue une préoccupation majeure, tout comme la nécessité de préserver les infrastructures critiques contre d'éventuelles cyberattaques pouvant causer des dégâts dans le monde physique.

Les menaces auxquelles nous faisons face aujourd'hui sont, pour la plupart, de nature transnationale et le seul moyen de les écarter, dans le monde physique comme dans l'espace virtuel, c'est par la coopération et par le dialogue à l'échelle internationale. En ce sens, si un État Membre n'est pas à l'abri, aucun autre ne l'est.

L'Équateur réaffirme donc son attachement aux règles existantes, telles que définies dans les rapports du Groupe d'experts gouvernementaux et les résultats du Groupe de travail à composition non limitée, qui viennent en complément du droit international. Ma délégation tient à souligner qu'aucun domaine ne peut être en dehors du champ d'application du droit international, notamment le droit international des droits humains et le droit international humanitaire, ce qui ne veut pas dire que la militarisation du cyberespace est acceptable.

Au contraire, l'Équateur défend l'utilisation du cyberespace à des fins exclusivement pacifiques. La Charte des Nations Unies interdisant l'emploi de la force, tout différend international dans le cyberespace doit être résolu par des moyens pacifiques.

Nous encourageons donc le renforcement de la confiance et des capacités et pour cela, nous pensons qu'une plateforme opérationnelle est nécessaire à la facilitation de la mise en œuvre du cadre existant par les États. Une telle plateforme pourrait correspondre à un programme d'action.

Nous préconisons et soutenons tout mécanisme qui favorise une plus grande coopération internationale afin de réduire le déséquilibre dans la capacité à appliquer les règles de comportement responsable des États.

Nous sommes également conscients de la contribution que les organisations régionales peuvent apporter au renforcement des capacités et à l'application de ces normes. Je cite en particulier le travail précieux de l'Organisation des États

américains dans ce domaine, notamment en matière de lutte contre la cybercriminalité et le terrorisme.

En conclusion, je rappelle la nécessité de préserver et de promouvoir une utilisation responsable des technologies numériques, qui est essentielle à la préservation de la stabilité et de la sécurité dans le cyberespace. Nous pensons également que les normes existantes doivent être renforcées pour tenir compte de l'évolution technologique rapide. Le Conseil de sécurité, pour sa part, devrait envisager des mécanismes visant à renforcer l'utilisation de la technologie comme moyen de consolidation de la paix, en complément des efforts classiques.

Annexe XXVIII

Déclaration de la Mission permanente de l'Égypte auprès de l'Organisation des Nations Unies

L'Égypte attache une grande importance aux aspects des technologies numériques liés à la sécurité internationale et prie instamment l'ONU de jouer un rôle central et prépondérant dans la promotion et l'élaboration de règles et de principes relatifs à l'utilisation de ces technologies par les États, dans le cadre d'un mécanisme inclusif et équitable auquel participent tous les États.

Un certain nombre d'États développent des cybercapacités pour d'éventuelles utilisations malveillantes et à des fins militaires offensives. La probabilité de l'utilisation des technologies numériques dans les futurs conflits entre États est près de devenir une réalité et le risque de cyberattaques malveillantes contre des infrastructures critiques est à la fois réel et sérieux. Cette nouvelle course aux armements a des répercussions considérables sur la paix, la sécurité et la stabilité internationales, d'autant plus que les frontières entre les armes conventionnelles et celles non conventionnelles continuent de s'effacer.

En outre, les technologies appropriées développées par les États sont transférées, copiées ou reproduites par des terroristes et des criminels. L'utilisation malveillante des technologies numériques par des organisations terroristes et criminelles constitue une menace sérieuse pour la paix et la sécurité internationales, notamment au vu des difficultés liées à l'attribution.

En vertu du droit international et de la Charte des Nations Unies, tous les États Membres doivent s'abstenir de poser, sciemment ou intentionnellement, tout acte qui endommage ou compromet l'utilisation et le fonctionnement des infrastructures critiques d'autres États, ainsi que de toute ingérence dans leurs affaires intérieures.

Il ne fait aucun doute que les aspects des technologies numériques liés à la sécurité internationale sont devenus trop importants et stratégiques pour qu'il n'y ait pas de règles contraignantes claires les régissant au niveau international. Un mécanisme inclusif au sein du système des Nations Unies est le moyen le plus pratique et le plus efficace pour la mise en place de dispositions qui soient équitables, complètes et susceptibles d'avoir des effets dans ce domaine.

L'ONU a déjà pris certaines mesures visant à établir un cadre normatif qui vient en complément des principes du droit international. Avec la récente adoption par consensus du rapport final du Groupe de travail à composition non limitée créé en application de la résolution 73/27 de l'Assemblée générale intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », l'ONU a déjà formulé les premiers éléments d'un cadre de prévention des conflits et de renforcement de la stabilité dans le cyberespace.

L'Assemblée générale a demandé aux États Membres de s'inspirer, pour ce qui est de l'utilisation des technologies numériques, des normes de comportement responsable des États contenues dans les rapports consécutifs des groupes d'experts gouvernementaux de la Première Commission. Toutefois, l'application de ces normes limitées reste, au mieux, assez faible, notamment en raison de leur caractère non contraignant et de l'absence de tout mécanisme de suivi.

Le succès du Groupe de travail à composition non limitée, qui est le premier mécanisme inclusif sur ce sujet important, et la création d'un nouveau groupe de travail de même nature en application de la résolution 75/240 de l'Assemblée générale représentent des progrès prometteurs vers un accord possible sur des visions communes importantes entre les États Membres sur un certain nombre d'aspects clés.

La mise place de mécanismes inclusifs au sein du système des Nations Unies, principalement sous les auspices de l'Assemblée générale, constituent le moyen le plus efficace d'établir des dispositions équitables, complètes et efficaces dans ce domaine. Pour sa part, le Conseil de sécurité est invité à tenir compte des possibilités offertes par les technologies émergentes lorsqu'il examine des sujets tels que le maintien de la paix et la lutte contre le terrorisme. Néanmoins, le Conseil ne devrait pas servir d'organe législatif qui tente de fixer des normes et des règles au nom des États Membres sur des questions qui nécessitent impérativement des procédures inclusives et transparentes.

Les recommandations qui ont été approuvées par l'Assemblée générale par consensus peuvent constituer une source de règles politiquement ou juridiquement contraignantes, d'autant plus qu'elles découlent des principes du droit international et de la Charte des Nations Unies.

L'Égypte a également invité les États Membres à envisager la création d'une plateforme institutionnelle inclusive consacrée à la coopération internationale sur la préservation de l'utilisation des technologies numériques à des fins pacifiques et sur la limitation des risques y relatifs.

Si nous pensons que le droit international et les principes de la Charte s'appliquent à tous les domaines, y compris le cyberespace, nous pensons également qu'il urge de déterminer les principes précis qui obligent les États à avoir dans le cyberespace un comportement conforme au droit international et aux objectifs de la Charte des Nations Unies.

Dans un monde de plus en plus interconnecté, la solidité de tout régime international en matière de cybersécurité sera fonction de son maillon le plus faible. Heureusement, tous les acteurs s'accordent à estimer que les efforts de renforcement des capacités doivent être intensifiés et améliorés afin de prévenir les attaques potentielles contre les infrastructures critiques et de développer les capacités et les compétences techniques nécessaires dans les pays en développement. L'ONU devrait mener une action coordonnée pour apporter aux pays en développement l'assistance dont ils ont besoin.

Pour conclure, les technologies numériques comportent à la fois une multitude d'obstacles à surmonter et de chances à saisir. Par conséquent, nous soulignons qu'il urge de définir et d'élaborer des règles de comportement responsable des États afin d'accroître la stabilité et la sécurité dans l'environnement numérique mondial et d'empêcher que le cyberespace ne devienne une nouvelle arène pour les conflits et les courses aux armements.

Annexe XXIX

Déclaration de la Mission permanente d'El Salvador auprès de l'Organisation des Nations Unies

[Original : espagnol]

El Salvador remercie la délégation estonienne, qui assure la présidence du Conseil de sécurité pour le mois de juin 2021, d'avoir organisé ce débat public qui marque la première fois que le Conseil de sécurité aborde le thème de la cybersécurité comme une question de fond et dans un format formel. Cette initiative est une mesure très importante qui permet à cet organe de s'acquitter de l'engagement international d'examiner au niveau multilatéral les cybermenaces existantes et potentielles.

Le développement des technologies numériques offre une occasion importante de promouvoir le développement économique et social des États. Cependant, ces systèmes d'information sont vulnérables face aux attaques de personnes qui tentent de manipuler ces réseaux de communication à des fins idéologiques ou pour leur propre bénéfice. Étant donné que les criminels et les terroristes tirent parti des technologies numériques pour atteindre leurs objectifs, il est nécessaire de déployer des efforts et des ressources pour travailler sur des lignes directrices spécialisées en vue de l'élaboration et de la mise en œuvre de normes communes permettant de prévenir ces délits, tout en facilitant l'application de la justice à ceux qui contreviennent à ces normes.

À cet égard, nous soulignons l'importance des instruments internationaux et régionaux relatifs à la lutte contre la cybercriminalité, ainsi que les progrès réalisés dans ce domaine, comme la création du Groupe de travail à composition non limitée chargé d'élaborer une convention internationale globale sur la lutte contre l'utilisation abusive des technologies numériques à des fins criminelles.

El Salvador se félicite des efforts déployés par les États Membres de l'ONU pour lutter contre le terrorisme dans le cadre du programme international pour la paix et la sécurité. Toutefois, nous constatons que, parmi les instruments internationaux contraignants dans ce domaine, on ne trouve toujours pas une mention explicite du cyberespace. C'est une lacune que nous devons corriger ensemble le plus rapidement possible. Ma délégation salue les efforts déployés par le Conseil de sécurité pour examiner minutieusement cette menace grave, en vue de lui trouver des solutions efficaces. Elle invite instamment cet organe de l'ONU à poursuivre ces efforts, en laissant de côté tout intérêt politique ou tout autre intérêt, en restant concentré sur la prévention de nouveaux conflits et de la création de scénarios propres à les aggraver.

El Salvador rappelle la résolution 58/199, adoptée par l'Assemblée générale en 2004, dans laquelle on énumère les éléments des infrastructures critiques d'un État qui, en raison de l'interdépendance technologique croissante, sont exposés à des menaces de plus en plus nombreuses et variées. Dans cette résolution, on reconnaît également que les faiblesses des infrastructures critiques donnent lieu à de nouvelles préoccupations en matière de sécurité.

En outre, afin de créer les conditions permettant de progresser vers l'objectif général de la paix et de la sécurité internationales, la pleine réalisation des droits humains et le développement économique et social, nous pensons que le cadre prévu par la résolution 58/199 de l'Assemblée générale devrait être élargi pour répondre à la nécessité de préserver les activités d'infrastructures critiques des cyberattaques, en plus des efforts actuellement déployés en vue d'empêcher que le cyberespace ne devienne une plateforme de propagande pour la radicalisation, le recrutement et la collecte de fonds pour des activités criminelles.

Le monde continue de faire face à l'un des plus grands défis depuis la création de cette Organisation. L'apparition de la pandémie de la maladie à coronavirus 2019 (COVID-19) a mis au jour les faiblesses des systèmes essentiels des États. Nous avons vu comment, pendant la pandémie de COVID-19, les cyberattaques contre les systèmes de santé des pays se sont multipliées, mettant en danger la vie de millions de personnes et touchant directement les populations et les secteurs les plus vulnérables. Nous profitons de cette occasion pour condamner les cyberattaques qui ont pris pour cible l'Organisation mondiale de la Santé et les tentatives de hameçonnage qui ont eu lieu ces derniers mois. Il ne fait aucun doute que l'interconnectivité accrue signifie que ces attaques pourraient se multiplier dans les années à venir.

L'utilisation malveillante des technologies numériques s'est étendue ces derniers mois aux cyberattaques contre les secteurs de l'énergie, de la finance et de l'approvisionnement alimentaire, qui sont, entre autres secteurs, très vulnérables aux cyberattaques. De même, nous avons assisté à une augmentation des activités de désinformation visant à influencer la perception des gouvernements et des institutions, des actions qui ont une forte capacité à délégitimer le travail de ceux-ci, ce qui a entraîné un climat d'instabilité et des conflits sociaux.

Il est donc impératif de continuer à travailler sur la prévention de ces activités et sur une codification du droit international visant à empêcher une utilisation abusive de l'informatique, en reconnaissant l'interdépendance avec le droit international humanitaire existant, y compris dans le domaine des cyberopérations pendant les conflits armés.

Ma délégation insiste sur l'importance de travailler sur la base du consensus, sans intention d'imposer aux États des solutions qui ne sont pas compatibles avec leurs réalités, et de veiller à ce que les progrès réalisés par l'Assemblée générale, grâce aux différents accords consensuels des groupes d'experts gouvernementaux et du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale ; nous espérons que cela sera pris en compte. En particulier, nous nous félicitons de l'adoption par consensus, en 2021, de l'accord du Groupe de travail à composition non limitée, auquel sont parties les 193 États Membres de l'ONU, y compris les 15 membres du Conseil de sécurité, et d'autres parties concernées.

El Salvador espère contribuer de manière constructive aux travaux du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui mènera ses travaux de fond au cours de la période 2021-2025, et salue le travail effectué par le Représentant permanent de Singapour auprès de l'Organisation des Nations Unies, Burhan Gafoor, en sa qualité de président désigné de ce mécanisme.

La délégation salvadorienne souligne le rôle fondamental des organisations régionales, du secteur privé, de la société civile, des milieux universitaires, et d'autres secteurs concernés, dans la prévention de ces menaces et la lutte contre celles-ci. Elle estime qu'il urge de continuer à travailler au renforcement des mécanismes de coopération régionale et internationale visant à prévenir et à combattre ces menaces, par un échange dynamique d'informations et de meilleures pratiques, le renforcement des capacités, la normalisation des cadres juridiques et le recours aux technologies numériques pour le développement et la lutte contre la criminalité organisée.

Annexe XXX

Déclaration du Chef de la Délégation de l'Union européenne auprès de l'Organisation des Nations Unies, M. Olof Skoog

C'est un honneur pour moi de contribuer au débat public sur la cybersécurité au nom de l'Union européenne et de ses États membres.

La Turquie, la République de Macédoine du Nord*, le Monténégro* et l'Albanie*, pays candidats, et la Bosnie-Herzégovine, pays du processus de stabilisation et d'association et candidat potentiel, ainsi que l'Ukraine et la République de Moldova s'associent à cette déclaration.

Tout d'abord, nous remercions l'Estonie d'avoir organisé ce débat public sur un sujet crucial, alors que les cyberactivités malveillantes ne cessent de se multiplier et que les difficultés à surmonter sont de plus en plus grandes en matière de sécurité et de stabilité internationales dans le cyberespace, en particulier dans les circonstances de la pandémie que nous traversons.

Le numérisation a un impact de plus en plus important sur notre sécurité, nos économies et nos sociétés en général, créant à la fois des opportunités et des problèmes. Les transports, l'énergie et la santé, les télécommunications, la finance, la sécurité, le processus démocratique et les domaines de l'espace et de la défense dépendent tous fortement de réseaux et de systèmes d'information, qui sont de plus en plus interconnectés.

À cet égard, nous sommes particulièrement inquiets de la multiplication récente des cyberactivités malveillantes qui prennent pour cible des prestataires essentiels dans le monde entier, notamment dans le secteur des soins de santé, et qui compromettent la disponibilité, la sécurité et l'intégrité des produits et services liés aux technologies de l'information et des communications ainsi que, par conséquent, la continuité des opérations, chose qui risque d'avoir d'autres retombées et des effets systémiques et accroître les risques de conflit.

Nous nous félicitons donc de l'occasion qui nous est offerte d'examiner cette question importante au Conseil de sécurité, qui a la responsabilité principale du maintien de la paix et de la sécurité internationales. C'est l'occasion de souligner un certain nombre de problèmes à surmonter, de rappeler les réalisations accomplies à ce jour par la famille des Nations Unies et de faire un tour d'horizon des moyens d'aborder ces questions au sein des Nations unies.

À cet égard, l'Union européenne et ses États membres se félicitent des rapports importants adoptés par consensus par le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (Groupe de travail à composition non limitée), qui a été créé récemment, et le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace.

Ces rapports contribuent beaucoup à faire mieux comprendre les enjeux et à accroître notre capacité de prévenir les cybermenaces et les cyberactivités malveillantes, d'y répondre et de s'en relever. Cela est indispensable, car le manque de sensibilisation et de capacités constitue une menace en soi, tous les pays étant de plus en plus dépendants des TIC.

Il est donc essentiel d'accroître la cyberrésilience mondiale, qui réduit la capacité des acteurs malintentionnés à utiliser les TIC à des fins malveillantes. Cela

* La République de Macédoine du Nord, le Monténégro, la Serbie et l'Albanie font toujours partie du processus de stabilisation et d'association.

permet également aux États de prendre les précautions et les mesures voulues face aux acteurs qui mènent de telles activités depuis leur territoire, conformément au droit international et aux rapports adoptés par consensus en 2010, 2013, 2015 et 2021 par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le cadre de la sécurité internationale.

Les rapports du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée établissent des points de repère pour la prévention des conflits, la coopération et la stabilité dans le cyberespace, notamment en réaffirmant l'importance de l'application du droit international et en examinant les normes relatives au comportement responsable des États et les moyens d'accroître la confiance dans le cyberespace et de renforcer les cybercapacités.

L'Union européenne et ses États membres réaffirment que tout cadre stratégique pour la prévention des conflits, la coopération et la stabilité dans le cyberespace doit être fondé sur le droit international existant, qui comprend la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international des droits humains, comme l'affirme l'Assemblée générale depuis 2013.

Mieux comprendre l'application du droit international au cyberespace, c'est réduire les malentendus et renforcer la responsabilité effective dans ce domaine. Les membres de l'ONU devraient continuer de faire progresser et de mettre en œuvre ce cadre stratégique afin de promouvoir la sécurité et la stabilité internationales dans le cyberespace.

Ainsi, de l'avis de l'Union européenne et de ses États membres, le droit international humanitaire est pleinement applicable au cyberespace dans le contexte des conflits armés. Nous réaffirmons qu'il ne faut voir en aucun cas dans son application au cyberespace la légitimation d'utilisations de la force contraires à la Charte des Nations Unies. Le droit international humanitaire établit des protections fondamentales pour ceux qui ne participent pas ou plus à des hostilités, s'agissant entre autres de protéger les civils contre les effets des hostilités et les combattants contre les souffrances inutiles. Il impose également des limites aux moyens et aux méthodes de combat qui sont admissibles, y compris ceux qui sont nouveaux.

Deuxièmement, l'adhésion aux normes relatives au comportement responsable des États est de la plus haute importance. L'ensemble des normes convenues traduit les attentes partagées de la communauté internationale et établit ainsi des points de référence pour le comportement responsable des États. Ces normes permettent à la communauté internationale d'évaluer les activités et les intentions des États afin de prévenir les conflits et de favoriser la stabilité et la sécurité dans le cyberespace.

Troisièmement, les mesures de confiance ayant trait au cyberespace constituent un moyen pratique de prévenir les conflits. Grâce à la coopération et au partage d'informations, les mesures de confiance prises au niveau régional ont permis de réduire le risque de malentendu, d'escalade et de conflit qui peut résulter des incidents liés aux TIC.

En dernier lieu, le cadre stratégique doit tenir compte de la question importante du renforcement des capacités. Nous soutenons activement l'appel qui a été lancé pour améliorer la cohérence des activités de renforcement des capacités dans l'utilisation des TIC pour réduire la fracture numérique, notamment dans le cadre des nombreuses initiatives que nous menons avec des partenaires du monde entier.

L'Union européenne contribue au renforcement des cybercapacités au moyen de ses instruments de financement extérieur, qui servent à financer divers programmes menés dans le monde entier, notamment en Afrique, en Asie et en Amérique latine, ainsi que dans les pays voisins de l'Union européenne et dans les Balkans

occidentaux. Concrètement, l'Union européenne investit actuellement dans des activités menées dans le monde entier pour contribuer à leur mise en œuvre en coopération avec ses partenaires de réalisation, dans le cadre de projets tels que Cyber Resilience for Development, Glacy+, EU Cyber Direct et l'initiative visant à renforcer la coopération en matière de sécurité en Asie et avec les partenaires asiatiques.

Afin d'appeler l'attention sur le cadre stratégique pour la prévention des conflits, de la coopération et de la stabilité dans le cyberespace, l'Union européenne continuera de promouvoir les comportements responsables dans le cyberespace. Dans cette optique, elle et ses États membres sont attachés au règlement des différends internationaux par des moyens pacifiques, y compris lorsque ces différends surviennent dans le cyberespace.

Créer un cadre pour mener une diplomatique commune s'inscrit donc dans l'approche de l'Union européenne en matière de cyberdiplomatie, l'objectif étant de contribuer à prévenir les conflits, à atténuer les menaces de cybersécurité et à accroître la stabilité des relations internationales. Afin de mettre en place et de préserver un cyberespace ouvert, libre, stable et sûr, l'Union européenne continuera d'utiliser sa boîte à outils cyberdiplomatique et de coopérer à cette fin avec ses partenaires internationaux.

Compte tenu de la nature complexe du cyberespace, il est de la plus haute importance que les États et l'ensemble des parties prenantes s'attaquent sans attendre aux difficultés créées par cyberespace, qu'ils améliorent la coopération et qu'ils renforcent leurs capacités. Il nous incombe également au premier chef de permettre à toutes les parties prenantes d'assumer leur responsabilité de faire progresser la mise en place d'un cyberespace ouvert, libre, sûr et stable, fondé sur les droits humains, les libertés fondamentales, la démocratie et l'état de droit, et de soutenir leurs efforts. L'approche de l'Union européenne en matière de cyberdiplomatie tient également compte de l'importance des questions de genre, afin de réduire la « fracture numérique entre les genres » et de promouvoir la participation effective et réelle des femmes aux processus décisionnels qui intéressent l'utilisation des TIC dans le contexte de la sécurité internationale.

Pour renforcer la coopération, nous pensons que l'ONU a un rôle central à jouer dans l'application des résultats obtenus à ce jour. Pour que les diverses parties prenantes puissent mener un débat multilatéral efficace afin de faire progresser la paix et la sécurité dans le cyberespace, il est manifestement nécessaire de faire progresser le cadre de l'ONU pour un comportement responsable des États dans le cyberespace. Avec 53 États Membres de l'ONU, l'Union européenne propose d'établir un programme d'action pour favoriser le comportement responsable des États dans le cyberespace.

En prenant pour point de départ les acquis déjà approuvés par l'Assemblée générale, le programme d'action créerait au sein de l'ONU un mécanisme permanent de coopération et d'échange de bonnes pratiques. Il permettrait de promouvoir les programmes de renforcement des capacités adaptés aux besoins tels que définis par les États bénéficiaires. Il établirait également un mécanisme institutionnel à l'ONU pour améliorer la coopération avec d'autres parties prenantes, telles que les acteurs du secteur privé, du monde de la recherche et de la société civile, en ce qui concerne les différentes responsabilités dont ils doivent s'acquitter, respectivement, pour que l'environnement numérique reste ouvert, libre, sûr, stable, accessible et pacifique.

Sachant que le mécanisme en question serait permanent et axé sur l'action, notre proposition nous semble opportune et digne d'être examinée plus avant par la communauté internationale. Le mécanisme établirait des bases solides et concrètes en

vue de poursuivre les travaux sur le cadre stratégique pour la prévention des conflits, la coopération et la stabilité dans le cyberespace, ainsi que de garantir que les États soient en mesure de tirer parti des avantages d'un cyberespace mondial, ouvert, stable et sûr.

Annexe XXXI

Déclaration de la Mission permanente de la Géorgie auprès de l'Organisation des Nations Unies

Nous tenons à exprimer notre gratitude à l'Estonie, qui a assuré la présidence, d'avoir organisé aujourd'hui le débat de haut niveau sur cette question importante, ainsi qu'à remercier les intervenants.

La Géorgie s'emploie depuis longtemps à mettre en place un cyberespace responsable et éthique, notamment en matière de cybersécurité et de résilience, en créant des cadres complets pour un environnement numérique sûr, fiable et digne de confiance, dans l'intérêt de l'ensemble de la nation. Au cours de la dernière décennie, nous avons établi les fondements juridiques nécessaires en matière d'information et de cybersécurité et recensé les aspects essentiels des systèmes d'information, adopté et appliqué deux stratégies de cybersécurité assorties de plans d'action, et lancé le processus d'adoption de notre troisième stratégie nationale de cybersécurité.

Toutefois, comme nous le savons tous, outre les possibilités majeures qu'il crée sur le plan économique et social et en matière d'innovation et de développement, le cyberespace est à l'origine de nouveaux types de menaces pour la sécurité. Ces dernières années, nous avons vu le cyberespace utilisé non seulement à des fins de terrorisme, de fraude et de criminalité, mais aussi comme un puissant outil de guerre hybride et d'ingérence dans les affaires intérieures des États.

Malheureusement, les moyens de guerre hybride sont également devenus de puissants instruments pour certains États qui s'en servent dans leur intérêt national. Le présent organe n'ignore pas que la Géorgie a une longue et douloureuse expérience de la gestion des menaces hybrides émanant de l'un de ses membres permanents. La Fédération de Russie mène une guerre hybride contre la Géorgie depuis le début des années 90 et n'a jamais cessé de tenter de porter atteinte à la souveraineté, à l'intégrité territoriale et aux aspirations européennes et euro-atlantiques de notre pays.

La liste des incidents est longue. En août 2008, pendant l'agression militaire de grande envergure de la Russie contre la Géorgie, nous avons assisté au premier cas de cyberattaque massive menée parallèlement à une agression armée. En 2019, une cyberattaque de grande ampleur a été lancée contre les sites Web, les serveurs et d'autres systèmes informatiques de l'administration de la Présidence de la Géorgie, des tribunaux, de diverses assemblées municipales, d'organes de l'État, d'organisations du secteur privé et de médias. L'enquête conduite par les autorités géorgiennes en coopération avec leurs partenaires a permis de conclure que la cyberattaque avait été planifiée et exécutée par la Division principale de l'État-major général des Forces armées de la Fédération de Russie.

Malheureusement, alors même que la communauté internationale lutte contre la pandémie de maladie à coronavirus (COVID-19), la Fédération de Russie tente encore d'obtenir des résultats politiques en intensifiant la guerre de propagande contre l'une des institutions géorgiennes les plus efficaces de la lutte contre la propagation du coronavirus : le centre Richard Lugar pour la recherche en santé publique. Les accusations de la Russie contre ce laboratoire exceptionnel, qui a été créé pour identifier et traiter les épidémies comme la pandémie que nous traversons, sont un exemple typique de campagne de désinformation et de propagande.

Aujourd'hui, nous sommes tous témoins de l'utilisation agressive que la Russie fait de ces moyens hybrides, non seulement dans notre région, mais également à l'échelle mondiale. Les principaux éléments de la boîte à outils russe sont les suivants : présence militaire, opérations d'information, cyberattaques, appui à des

groupes politiques agissant pour le compte de la Russie, ingérence dans les affaires intérieures et influence économique.

En conclusion, nous devons souligner que les cyberattaques et la guerre hybride contre des États souverains constituent de graves violations du droit international, de ses normes et de ses principes et qu'elles compromettent la paix et la sécurité internationales. Tout en réaffirmant notre volonté de continuer de renforcer la cybersécurité au niveau national et international, nous demandons également à la communauté internationale de prêter une plus grande attention aux activités malveillantes menées par la Fédération de Russie dans le domaine des technologies de l'information et des communications, en Géorgie et ailleurs.

Annexe XXXII

Déclaration de la Mission permanente de l'Allemagne auprès de l'Organisation des Nations Unies

Il y a un an et demi, la pandémie de maladie à coronavirus (COVID-19) s'est abattue sur le monde et nous a fait prendre conscience – brutalement – de la mesure dans laquelle les technologies numériques façonnent à la fois notre vie quotidienne et notre résilience économique. Dans le même temps, elle a impitoyablement exposé nos vulnérabilités. Les cyberattaques, notamment celles qui visent des infrastructures critiques, peuvent faire peser une menace sur la paix et la sécurité internationales, et l'Allemagne est convaincue qu'il s'agit d'un sujet important pour le Conseil de sécurité.

La paix et la sécurité internationales sont soumises à différentes pressions : tout d'abord, les activités cybercriminelles compromettent la fiabilité et la crédibilité de technologies qui sont désormais indispensables au fonctionnement de nos économies, de nos États et de nos sociétés modernes dans leur ensemble. Pour ne citer que quelques exemples, on constate depuis le début de la pandémie une forte augmentation des attaques par déni de service, des tentatives d'hameçonnage et de la diffusion de logiciels malveillants. On constate également de plus en plus d'attaques contre des infrastructures critiques en Europe et en Amérique du Nord et de cyberattaques utilisées comme moyen d'extorsion.

Deuxièmement, les cyberactivités malveillantes soutenues par des États à des fins d'espionnage, de sabotage, de désinformation, de déstabilisation ou de gain financier portent atteinte à la fois à la confiance internationale et aux mécanismes coopératifs d'atténuation des conflits, compromettant ainsi la sécurité dans le monde entier.

Troisièmement, la société civile dans son ensemble et les défenseurs des droits humains en particulier sont soumis à une pression de plus en plus forte dans le cyberespace. L'espace de liberté d'expression, de transparence et de communication authentique – que l'Internet est censé rendre possible – ne cesse de se réduire.

Face à ces menaces de plus en plus graves, il faut adopter une approche reposant sur plusieurs piliers : le premier consiste à renforcer notre résilience au niveau national et international. Cela passe par l'amélioration des infrastructures techniques, des capacités politiques et juridiques, ainsi que par le renforcement de la coopération internationale.

Le deuxième pilier consiste à définir et à faire progresser notre conception commune du comportement responsable des États dans le cyberespace et à fixer les lignes rouges à ne pas franchir. Nous devons donc défendre les acquis du Groupe de travail à composition non limitée et du Groupe d'experts gouvernementaux et faire progresser l'élaboration de normes relatives au comportement responsable des États.

La position de l'Allemagne est la suivante : le droit international, y compris la Charte des Nations Unies et le droit international humanitaire, s'applique en ligne aussi bien que hors ligne. Les États devraient s'abstenir strictement de soutenir toute activité liée aux technologies de l'information et de la communication (TIC) qui serait contraire aux obligations que leur impose le droit international – notamment en raison du risque qu'il y aurait de créer et d'aggraver des tensions entre États. Les activités liées aux TIC ne doivent pas endommager intentionnellement les infrastructures critiques ni nuire d'aucune autre manière à leur utilisation ou à leur fonctionnement. En particulier, aucun acteur ne doit mettre en péril la disponibilité générale ni l'intégrité du noyau public d'Internet, qui est vital pour la stabilité du cyberespace. Nous appelons tous les États à observer strictement les obligations que leur impose

le devoir de précaution et à agir rapidement contre les acteurs qui mènent des cyberactivités malveillantes depuis leur territoire, conformément au droit international.

Afin d'alimenter les débats en cours sur le droit international et le cyberespace, l'Allemagne a publié un document d'orientation sur l'applicabilité du droit international au cyberespace, et nous encourageons les autres pays à faire de même.

Il ne suffit cependant pas de s'entendre sur les acquis communs. Il importe tout autant de réagir fermement aux comportements inacceptables. Différents instruments sont envisageables à cette fin, allant du dialogue et de l'échange aux déclarations politiques faites par des États ou des groupes d'États pour exposer et dénoncer les comportements irresponsables, ou pour imposer des sanctions aux personnes et entités responsables. Avec nos partenaires de l'Union européenne, nous avons mis en place un régime de sanctions en matière de cybercriminalité qui nous permet de réagir aux cyberattaques de manière ferme, efficace, ciblée et pleinement conforme au droit international. Nous avons utilisé cet instrument par le passé et nous n'hésiterons pas à y recourir de nouveau si notre sécurité est compromise. En outre, une culture favorable à l'attribution peut contribuer à renforcer le cadre normatif et la responsabilité effective dans le cyberespace.

Il est essentiel d'avoir des échanges suivis avec les acteurs de la société civile, du secteur privé et du monde universitaire pour accroître notre résilience dans le cyberespace et faire avancer la cause de la gouvernance d'Internet. L'action que nous menons doit permettre de tirer parti des compétences très abondantes qui existent en dehors des autorités publiques, afin de maintenir la paix et la sécurité internationales dans le cyberespace.

Annexe XXXIII

Déclaration de la Mission permanente de la Grèce auprès de l'Organisation des Nations Unies

Les technologies numériques contribuent profondément à la transformation des économies et des sociétés qui est en cours, en créant des possibilités importantes de croissance économique, ainsi que de développement durable et inclusif. Le cyberespace, en particulier, est devenu l'un des piliers de nos sociétés. Dans le même temps, la multiplication des comportements malveillants dans le cyberespace, notamment l'utilisation abusive que font certains acteurs étatiques et non étatiques des technologies de l'information et des communications (TIC), est à l'origine de nouveaux risques et problèmes. Ces comportements compromettent la croissance économique et peuvent avoir des conséquences déstabilisatrices en cascade qui accroissent les risques de conflit.

Nous soutenons donc fermement le cadre stratégique pour la prévention des conflits, la coopération et la stabilité dans le cyberespace qui a été approuvé par l'Assemblée générale, et soulignons qu'il faut focaliser notre action collective sur la mise en place des compétences et des capacités nécessaires pour bien faire face aux cybermenaces. La nécessité de la cyberrésilience mondiale est mise en évidence par la crise sanitaire mondiale que nous traversons et pendant laquelle nous avons observé des cybermenaces et des cyberactivités malveillantes visant le secteur des soins de santé.

La cyberrésilience mondiale réduit la capacité qu'ont les acteurs malintentionnés d'abuser des TIC en même temps qu'elle renforce celle qu'ont les États à réagir efficacement aux atteintes à la cybersécurité et à s'en relever. Dans le cadre des initiatives que nous avons prises récemment pour renforcer la résilience mondiale et mettre au point des mesures de coopération concrètes, nous sommes en train d'organiser un séminaire régional sur la cybersécurité avec des participants des Balkans occidentaux.

Grâce à notre participation active à des organisations internationales telles que l'ONU, l'OTAN et l'Organisation pour la sécurité et la coopération en Europe, nous cherchons à coopérer, à échanger des expériences et des bonnes pratiques et à contribuer dans toute la mesure possible à l'élaboration de moyens appropriés de faire face aux cybermenaces. En outre, en tant que membre de l'Union européenne, nous mettons en œuvre un cadre stratégique inclusif et pluridimensionnel pour la prévention des conflits et la stabilité dans le cyberespace. Dans l'Union européenne, la cybersécurité relève d'une action coordonnée que les États membres mènent collectivement, exemple précieux de coopération multilatérale qui n'a guère de précédent.

Nous sommes très attachés à la mise en place d'un cyberespace mondial, pacifique, sûr, ouvert, indépendant et régi par le droit international, où les droits humains, les libertés fondamentales et l'état de droit s'appliquent pleinement. Nous nous employons activement à mettre en commun nos expériences de l'application de normes et de mesures de confiance et à renforcer nos capacités en coopérant tant au niveau bilatéral que multilatéral, dans toutes les instances régionales et internationales auxquelles nous participons. Nous sommes résolus à participer activement aux autres débats qui seront tenus à l'ONU sur les questions de cybersécurité et nous réaffirmons notre volonté de travailler constructivement pour progresser.

Annexe XXXIV

Déclaration de la Mission permanente du Guatemala auprès de l'Organisation des Nations Unies

Le Guatemala remercie la délégation estonienne, qui a assuré la présidence du Conseil de sécurité, d'avoir organisé ce débat public sur une question qui est assurément de la plus haute importance pour les États. Le cyberespace est devenu un domaine central et indispensable de l'activité mondiale, et il est essentiel de le protéger en veillant au comportement responsable des États pour maintenir la paix et la sécurité internationales. Nous sommes convaincus que les réunions de ce type sont une excellente occasion pour nos pays d'échanger des avis et des principes de bonne pratique en ce qui concerne les différents niveaux de mise en œuvre des mesures dans ce domaine de plus en plus important.

Le monde fait face à plusieurs problèmes de sécurité qui sont aggravés par l'apparition de nouvelles menaces – notamment celles qui pèsent sur la cybersécurité. Lorsque l'on réfléchit aux cyberattaques qui ont été commises par le passé et à la multiplication de ce type d'attaques pendant la pandémie de maladie à coronavirus 2019 (COVID-19), la nécessité d'aborder ces problèmes saute aux yeux, d'autant plus qu'ils risquent de toucher les secteurs les plus vulnérables de notre société.

Les cybermenaces et les cyberattaques naissent et évoluent en fonction des diverses activités qui sont développées à la faveur de l'interconnexion de différents médias numériques, d'où une situation complexe face à laquelle tous les secteurs de nos pays doivent agir et coopérer, afin de développer des cadres techniques et juridiques qui renforcent la cybersécurité à l'échelle nationale et mondiale.

Comme dans tous les pays, les technologies de l'information et des communications (TIC) sont de plus en plus utilisées dans tous les pans de la société guatémaltèque. Cette évolution a permis aux échanges d'informations et aux communications de se développer dans une mesure sans précédent, mais elle entraîne aussi de nouveaux risques et menaces pour la sécurité de nos populations.

Dans ce contexte, ma délégation souhaite exprimer ses inquiétudes devant ces nouvelles technologies, notamment en raison des utilisations autres que civiles qui peuvent être faites du cyberespace et des réseaux numériques, y compris par des groupes criminels et terroristes. Il est extrêmement préoccupant que plusieurs États développent leurs capacités en matière de TIC à des fins militaires et que l'utilisation de ces technologies dans de futurs conflits soit de plus en plus probable.

Compte tenu de la complexité et de la nature interconnectée du cyberespace, le Guatemala estime que les gouvernements, le secteur privé, la société civile et le monde universitaire doivent agir de concert pour apporter des réponses complètes et équilibrées aux problèmes de cybersécurité. Il est de la responsabilité de tous ces secteurs de maintenir un cyberespace ouvert, libre, sûr et stable.

C'est pourquoi mon pays promeut les mesures de confiance et de transparence et apporte son soutien aux activités de renforcement des capacités, à l'échange d'informations et à la diffusion des meilleures pratiques, aux niveaux sous-régional, régional et international.

Ma délégation souhaite souligner l'importance cruciale de l'applicabilité du droit international au comportement des États dans le cyberespace, des normes facultatives et non contraignantes relatives au comportement des États applicables en temps de paix et de la mise en œuvre de mesures de confiance. En outre, ayant constaté les écarts qui existent d'un pays à l'autre en matière de cybersécurité et de défense, mon pays prête une attention particulière aux efforts de renforcement des

capacités, l'idée étant de parvenir à des conditions plus équitables qui concourraient à maintenir la paix et la sécurité internationales.

Le Guatemala est d'avis que les organisations régionales jouent un rôle indispensable dans le rétablissement de la paix sur le terrain. Il pourrait être très utile d'accroître leur présence dans le cyberespace, à l'échelle aussi bien régionale que mondiale, pour faire progresser la pérennisation de la paix par des moyens novateurs. Les organisations régionales et sous-régionales s'emploient à renforcer la sécurité des États, ce qui a beaucoup fait progresser la mise en œuvre de mesures de confiance concrètes dans les différentes régions de façon à améliorer la cybersécurité. Il ne fait aucun doute que, sans les contributions de ces organisations, moins d'efforts seraient faits pour prévenir les conflits et accroître la stabilité.

Notre stratégie nationale de cybersécurité a pour objectif principal de renforcer nos capacités, en créant l'environnement et les conditions nécessaires pour garantir la participation de la population ainsi que le développement et l'exercice des droits des personnes dans le cyberespace. Le Guatemala dispose en outre d'un centre d'intervention d'urgence en cas de cyberincident (CERT), qui assure des services dans les domaines suivants : audits en matière de cybersécurité, analyses des vulnérabilités et classification des alertes. Aussi bien la stratégie que le centre d'intervention ont été mis en place avec l'aide de l'Organisation des États américains.

En outre, le Guatemala élabore actuellement une loi sur la cybercriminalité, qui définit clairement les mesures à prendre et les types d'infractions en matière TIC, afin de contribuer à renforcer les capacités grâce à la coopération internationale, en favorisant la régularité de la procédure grâce à des protocoles bien définis pour le traitement des preuves numériques et la chaîne de suivi correspondante. Il convient par ailleurs de préciser que mon pays a l'honneur d'être un pays observateur de la Convention sur la cybercriminalité, qui vise à lutter contre les délits informatiques et les crimes sur Internet grâce à l'harmonisation des législations des différents pays, à l'amélioration des techniques d'enquête et au renforcement de la coopération entre les pays.

Ma délégation juge nécessaire de continuer de transformer et d'ajuster les législations nationales de façon harmonisée et de concevoir des systèmes qui permettent de déceler les cas probables d'infraction, d'enquêter à leur sujet et de poursuivre leurs auteurs, dans le cadre d'un dispositif qui protège les droits des personnes et qui réduit en même temps le risque que les réseaux informatiques soient utilisés dans l'objectif de compromettre la confidentialité, l'intégrité et la disponibilité des informations. Nous espérons que le débat d'aujourd'hui contribuera et servira de complément au processus d'élaboration de normes relatives au cyberespace qui se déroule à l'Assemblée générale, en particulier dans le cadre des travaux importants du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée créé pour la période 2021-2025.

Enfin, nous rappelons à tous les États qu'ils doivent utiliser les TIC pacifiquement et pour le bien commun de l'humanité, en favorisant le développement durable de tous les pays, quel que soit leur degré de développement scientifique et technologique.

Annexe XXXV

Déclaration du Chargé d'affaires de l'Indonésie auprès de l'Organisation des Nations Unies, de M. Mohammad Kurniadi Koba

Permettez-moi de remercier l'Estonie d'avoir convoqué cette réunion. Je tiens également à remercier la Haute-Représentante de son exposé fort utile.

Nous sommes de plus en plus dépendants à l'égard de la connectivité numérique, et les technologies de l'information et des communications (TIC) font désormais partie intégrante de notre vie quotidienne.

En outre, pendant la pandémie de maladie à coronavirus 2019 (COVID-19), les TIC ont permis aux secteurs public et privé d'assurer des services essentiels à la population.

À cet égard, il est essentiel de souligner que les cyberactivités malveillantes d'acteurs étatiques et non étatiques, en particulier celles qui visent les infrastructures critiques, risquent de mettre en péril la stabilité des pays ainsi que la paix et la sécurité internationales.

Dans ce contexte, l'Indonésie souhaite souligner les éléments suivants :

Premièrement, l'état de droit doit déterminer notre conduite en ce qui concerne l'utilisation des TIC ainsi que ses conséquences pour la paix et la sécurité internationales.

Les principes du droit international et la Charte des Nations Unies constituent les normes juridiques fondamentales qui encadrent l'utilisation que les États font des TIC, y compris pour réagir aux actes malveillants.

Tous les États doivent être guidés par le même ensemble de règles et de normes juridiques. Aucun d'entre eux ne doit pouvoir s'en affranchir.

En outre, l'Indonésie soutient les normes relatives au comportement responsable des États qui sont exposées dans la résolution 70/237 de l'Assemblée générale.

Tout en répondant au besoin de plus en plus grand qu'il y a de déterminer et de renforcer le cadre juridique international en cette matière, nous devons également chercher à combler les écarts entre les pays et les régions.

Il faut remédier aux écarts d'ordre technique, mais il est également impératif de renforcer les cadres politiques nationaux ainsi que l'application du droit international existant et des normes facultatives et non contraignantes dans le cyberespace.

Deuxièmement, les approches bilatérales, régionales et multilatérales ont toutes un rôle à jouer dans le renforcement de la confiance dans le cyberespace.

Les mesures de coopération bilatérales, régionales et multilatérales se renforcent les unes les autres de façon à faire progresser les connaissances et à accroître la stabilité dans le cyberespace, en particulier dans le domaine du renforcement des capacités et de la confiance.

Les mesures de renforcement de la confiance de l'Association des nations de l'Asie du Sud-Est (ASEAN) – à savoir la création de points de contact, l'échange régulier d'informations, le dialogue et la mise en commun des meilleures pratiques – ont contribué à la cybersécurité dans la région et au-delà, en particulier dans le cadre des travaux du Forum régional de l'ASEAN.

En outre, l'Indonésie souligne combien il est utile aux États de travailler réellement en partenariat avec des entités multipartites afin d'appliquer plus facilement le cadre pour les comportements responsables à leur utilisation des TIC.

À cet égard, il faut que les pays développés permettent aux pays en développement d'utiliser les TIC. Comme pour tous les autres problèmes de portée mondiale, l'action menée pour que les autres pays disposent des bons outils et des capacités nécessaires pour faire face aux menaces contribuera à la stabilité générale dans le domaine des TIC.

Troisièmement, l'ONU doit diriger l'action coordonnée visant à régler les conflits qui peuvent découler d'incidents liés aux TIC.

Le débat d'aujourd'hui est le premier que le Conseil consacre à l'impact des TIC sur le maintien de la paix et de la sécurité internationales.

Il témoigne d'un progrès important dans ce domaine à l'ONU.

À l'avenir, le Conseil devra anticiper les aggravations des menaces dans le cyberespace, ainsi que les incidents relatifs aux TIC qui risquent de conduire à une guerre majeure.

Nous soulignons combien il importe que les mesures prises par l'ONU soient coordonnées et synergiques. Le Conseil devrait continuer à agir pour maintenir la paix et la sécurité internationales, ainsi qu'à réagir aux conséquences humanitaires de l'évolution des TIC.

En même temps, le Conseil doit s'appuyer sur les normes et les règles qui ont été examinées et élaborées par l'Assemblée générale.

Permettez-moi de conclure en réaffirmant que l'Indonésie est résolue à faire progresser nos efforts communs pour prendre les mesures voulues face aux problèmes que pose l'utilisation des TIC pour le maintien de la paix et de la sécurité.

Annexe XXXVI

Déclaration du Comité international de la Croix-Rouge

Le Comité international de la Croix-Rouge (CICR) apprécie l'occasion qui lui est donnée de contribuer à ce débat public du Conseil de sécurité sur la question du maintien de la paix et de la sécurité internationales dans le cyberespace.

Au cours des deux dernières décennies, les cyberopérations hostiles sont devenues de plus en plus inquiétantes du point de vue du maintien de la paix et de la sécurité internationales. La numérisation des sociétés s'accompagne de l'augmentation des capacités militaires des États et d'autres acteurs. Aujourd'hui, la communauté internationale sait que « plusieurs États mettent au point des technologies numériques à des fins militaires » et que « la probabilité que ces technologies soient utilisées dans des conflits futurs entre États augmente »[10].

Compte tenu de cette réalité, le CICR souhaite rappeler les dommages que l'utilisation des cybertechnologies peut potentiellement causer aux êtres humains, et présenter ensuite les moyens par lesquels les États peuvent atténuer ces conséquences humanitaires négatives en prenant des mesures aux niveaux international et national.

Il est maintenant bien établi que des cyberopérations contre des infrastructures civiles critiques ont causé des dommages économiques importants, des perturbations dans les sociétés et des tensions entre les États. Dans le rapport final du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, tous les États ont reconnu que les cyberopérations contre les infrastructures critiques pouvaient avoir des conséquences humanitaires potentiellement désastreuses[11]. Bien qu'il ne soit pas en mesure de confirmer que des cyberopérations ont causé des pertes humaines, le CICR est préoccupé par les effets destructeurs de ces opérations, notamment l'interruption de l'approvisionnement en électricité ou en eau ou des services médicaux[12]. À tout moment, ce type d'opérations fait peser des risques graves sur les êtres humains. Notre expérience nous apprend cependant que la perturbation des infrastructures civiles critiques a des conséquences particulièrement graves dans les sociétés déjà affaiblies par un conflit armé.

Les conséquences humanitaires néfastes ne sont *pas* inévitables. Les États doivent prendre des mesures énergiques pour garantir que leur utilisation des cyberopérations pendant les conflits armés soit conforme aux règles existantes du droit international. De l'avis du CICR, cela passe par une action internationale et nationale.

Au niveau international, les États ont affirmé que le droit international s'appliquait à l'environnement numérique. Il s'agit avant tout des obligations des États en vertu de la Charte des Nations Unies, à savoir en particulier l'interdiction de l'emploi de la force et l'obligation de régler les différends internationaux par des moyens pacifiques. Depuis, le Groupe d'experts gouvernementaux a également noté que le droit international humanitaire s'appliquait uniquement en cas de conflit armé. Le groupe a rappelé « les principes juridiques internationaux établis, notamment, lorsqu'ils sont applicables, les principes d'humanité, de nécessité, de proportionnalité et de distinction notés dans le rapport de 2015 », et il a reconnu « qu'il convenait d'examiner plus avant de quelle manière et à quel moment ces principes

---

[10] Groupe de travail à composition non limitée, Rapport final, 2021, par. 16 ; Groupe d'experts gouvernementaux, Rapport final, 2021, par. 7.

[11] Groupe de travail à composition non limitée, Rapport final, 2021, par. 18.

[12] Disponible à l'adresse www.icrc.org/en/document/potential-human-cost-cyber-operations (en anglais).

s'appliquaient à l'utilisation des technologies numériques par les États et a souligné que le rappel de ces principes ne légitimait ni n'encourageait en aucun cas les conflits »[13]. Le CICR adhère pleinement à ce point de vue : les cyberopérations menées pendant les conflits armés ne se déroulent pas dans un « vide juridique » ni une « zone grise », mais sont soumises aux principes et règles établis du droit international humanitaire.

Afin de garantir la bonne compréhension et l'application effective du droit international humanitaire, le CICR juge souhaitable d'étudier plus avant les modalités et les conditions d'application de ce domaine du droit. Pour éviter les conséquences humanitaires néfastes et la perturbation des sociétés, nous demandons aux États d'interpréter et d'appliquer les règles et les principes du droit international humanitaire en tenant compte des caractéristiques spécifiques de l'environnement numérique. Certaines questions essentielles concernant la protection de la vie civile appellent un examen plus approfondi et un positionnement clair de la part des États. Par exemple, dans un monde où la place des données ne cesse de grandir, il devrait être prioritaire pour les États de convenir que les données civiles bénéficient d'une protection contre les attaques, tout comme les documents civils en format papier. En outre, les États devraient affirmer que les cyberopérations qui endommagent des biens civils en perturbant leur fonctionnement sont soumises à toutes les règles du droit international humanitaire qui ont trait à la conduite des hostilités[14].

Il importe certes de continuer d'étudier les limites que le droit international impose aux cyberopérations pendant les conflits armés et de s'entendre à ce sujet, mais les règles en question ne deviendront effectives que si elles sont mises en application au niveau national. En s'appuyant sur ses échanges avec des acteurs et experts du domaine militaire, le CICR a recensé un certain nombre de moyens clés par lesquels les États peuvent et doivent éviter que les opérations militaires causent des dommages aux civils pendant les conflits armés[15]. Aujourd'hui, nous souhaitons mettre l'accent sur quatre de ces mesures :

– Premièrement, chaque État est responsable de l'ensemble de ses organes qui participent à des cyberopérations et des autres acteurs qui agissent sur ses instructions ou sous sa direction ou son contrôle. Les États doivent veiller à ce que tous ces acteurs respectent le droit international humanitaire.

– Deuxièmement, les États doivent mettre en place des processus internes clairs pour garantir que toute utilisation de moyens ou méthodes de guerre cybernétiques soit conforme au cadre juridique applicable.

– Troisièmement, les États ont l'obligation de prendre toutes les précautions possibles pour éviter ou au moins réduire au minimum les dommages indirects causés aux civils lorsqu'ils mènent des attaques, y compris par des moyens et méthodes de guerre cybernétiques. Dans l'environnement numérique, il peut s'agir de prendre des mesures techniques telles que la mise en place de périmètres de systèmes, de périmètres de géoblocage ou de moyens d'arrêt d'urgence[16].

---

[13] Groupe d'experts gouvernementaux, Rapport final, 2021, par. 71 f).

[14] Voir aussi Comité international de la Croix-Rouge (CICR), « Le droit international humanitaire et les cyberopérations pendant les conflits armés », document de position, 2019.

[15] CICR, Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts, 2021.

[16] Les périmètres de système servent à empêcher les logiciels malveillants de s'exécuter à moins qu'il n'y ait une correspondance précise avec le système cible ; les périmètres de géoblocage empêchent les logiciels malveillants d'opérer en dehors d'une certaine plage d'adresses IP ; les dispositifs d'arrêt d'urgence permettent de désactiver les logiciels malveillants après un certain laps de temps ou lorsqu'ils sont activés à distance.

– Quatrièmement, les États ont l'obligation de mettre en place des mesures pour protéger la population civile contre les risques résultant des cyberopérations militaires. Certaines de ces mesures devront peut-être déjà être appliquées en temps de paix.

En conclusion, le CICR félicite les États Membres de s'efforcer de faire progresser le dialogue et l'entente au niveau international au sujet du coût humain potentiel des cyberopérations et des mesures destinées à prévenir et à atténuer les préjudices humains. Nous sommes d'avis que le droit international humanitaire doit être pris en compte dans ces débats, auxquels nous sommes prêts à contribuer si nos compétences sont requises.

Annexe XXXVII

Déclaration du Directeur exécutif des Services de police de l'Organisation internationale de police criminelle (INTERPOL)

Introduction

La cybercriminalité représente un enjeu mondial à l'ère du numérique. Son impact va bien au-delà de ce qui est signalé ou détecté : elle influe sur la vie quotidienne de plus de 4,5 milliards de personnes en ligne. L'accroissement de la place accordée à l'environnement numérique a créé de nouvelles possibilités d'activités illégales dans le cyberespace. S'étant tournée vers les gouvernements, les entreprises, les infrastructures clés et même les hôpitaux, la cybercriminalité représente aujourd'hui un défi formidable pour la sécurité dans le monde entier. Compte tenu de la croissance rapide de ce problème tant sur le plan de son ampleur que de sa gravité, l'Organisation internationale de police criminelle (INTERPOL) a fait de la lutte contre la cybercriminalité une priorité.

Organisation intergouvernementale mondiale et neutre, INTERPOL possède des connaissances sur le droit international, les normes, les mesures de confiance et les efforts de renforcement des capacités visant à maintenir la paix et la sécurité dans le cyberespace. Compte tenu de l'objectif de ce débat public, qui est de mieux comprendre les risques de plus en plus grands qui découlent des activités malveillantes menées dans le cyberespace, INTERPOL soumet la présente déclaration écrite au Conseil de sécurité pour contribuer à mettre en place un cyberespace pacifique et sûr. Nous y présentons l'évolution récente de la cybercriminalité et de ses incidences, ainsi que les mécanismes mondiaux et les outils dont disposent les 194 pays membres d'INTERPOL pour faire face à ces problèmes pressants.

Les cybermenaces actuelles et émergentes

L'année dernière, INTERPOL a analysé toute une série de cybermenaces. L'évaluation qu'elle a conduite récemment a fait ressortir que la pandémie de maladie à coronavirus (COVID-19) avait ouvert de nouvelles voies aux cybercriminels pour mener diverses activités illégales en ligne, dans toutes les régions. Les principales menaces que nous avons observées sont l'extorsion par logiciel rançonneur, la compromission de courriers électroniques professionnels, les opérations illégales de collecte de données, la désinformation et la réapparition d'anciens types de logiciels malveillants, modifiés pour tirer parti de la pandémie mondiale.

Par ailleurs, nous avons constaté que les attaques ciblaient de plus en plus souvent les grandes entreprises, les États et les infrastructures critiques [17]. Les cybercriminels et les fraudeurs exploitent les besoins fondamentaux et les angoisses de la société. Depuis mars 2020, INTERPOL a reçu un certain nombre de demandes de ses pays membres pour les aider à faire face à des attaques par logiciel rançonneur lancées contre des hôpitaux et d'autres institutions en première ligne de la lutte contre le coronavirus[18]. En attaquant ces infrastructures critiques qui jouent un rôle crucial dans la riposte à l'épidémie, les criminels ont pu maximiser les dégâts et les gains financiers.

---

[17] INTERPOL, Rapport d'évaluation de l'impact de COVID-19 sur la cybercriminalité, consulté sur https://www.interpol.int/fr/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf.

[18] https://www.interpol.int/fr/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.

Les attaques par logiciel rançonneur ne sont pas nouvelles, mais il s'agit de la forme de cybercriminalité qui croît le plus rapidement. Les logiciels de ce type constituent une activité très attrayante et très lucrative pour les cybercriminels, compte tenu du recours à la double extorsion et à la fourniture de ces logiciels à titre de service. Nous avons également constaté que ces attaques n'étaient pas limitées géographiquement, ce qui suggère que les criminels étendent leur champ d'action aux institutions de tout type et du monde entier. Par exemple, des logiciels de la même famille ont été utilisés en Europe, pour paralyser un hôpital, et en Asie.

En outre, nous avons constaté que des personnes étaient victimes de fraudes complexes en Europe et que les sommes extorquées étaient acheminées en quelques heures jusqu'en Afrique occidentale et en Asie du Sud-Est. Des violations massives de données continuent également de se produire, causant des pertes financières importantes à des entreprises des quatre coins du monde. Dans le même temps, les cybercriminels se dissimulent grâce au darknet, qui garantit un accès anonyme et intraçable. Cela rend d'autant plus importantes les notices INTERPOL, en particulier la notice mauve, qui permet aux pays membres d'échanger des informations sur le modus operandi de ces systèmes frauduleux [19]. L'objectif est de diffuser ces informations cruciales avant que l'attaque suivante ne survienne.

En outre, la convergence entre la cybercriminalité et la criminalité financière est un problème complexe. Les pratiques qui en résultent comportent plusieurs phases, de la cyberattaque à l'exploitation des données, qui sont suivies des phases de blanchiment d'argent par empilage et enfin de l'encaissement. L'utilisation de crypto-monnaies dans le processus entrave également la possibilité d'agir rapidement et efficacement. Compte tenu de cette complexité, il est nécessaire de mettre en place un modèle opérationnel commun réunissant les capacités de différents services spécialisés des forces de l'ordre pour mieux lutter contre la fraude liée à la cybersécurité et le blanchiment d'argent. Afin d'offrir une gamme complète de services de soutien opérationnel et analytique dans ce domaine, INTERPOL a créé un groupe de travail mondial sur la criminalité financière à la fin de 2020.

Mécanisme mondial d'atténuation des cybermenaces

En effet, la coopération policière internationale est essentielle à la sûreté et à la sécurité d'un monde extrêmement interconnecté. Comme l'a souligné l'ONUDC dans son étude approfondie sur la cybercriminalité, INTERPOL joue un rôle précieux dans la facilitation de la coopération entre les services de police[20]. À l'appui de ses 194 pays membres, elle a pour mandat de faciliter la coopération transfrontière entre les services de maintien de l'ordre et, selon les besoins, de soutenir les organisations, autorités et services gouvernementaux et intergouvernementaux qui ont pour mission de prévenir ou de combattre la criminalité, dans les limites des lois en vigueur dans les différents pays et dans l'esprit de la Déclaration universelle des droits de l'homme.

Grâce à sa neutralité et à sa présence dans le monde entier, INTERPOL est particulièrement bien placée pour diriger et coordonner l'action mondiale des services de maintien de l'ordre face à la cybercriminalité. Elle permet aux services de maintien de l'ordre du monde entier de partager des informations sur les acteurs de la cybercriminalité et des cybermenaces, et met à leur disposition une grande diversité de compétences et de services de conseil technique et de soutien opérationnel. Forte de ce rôle unique qui est le sien, INTERPOL a promu la coopération policière internationale dans le cadre de divers mécanismes stratégiques de l'ONU, tels que le

[19] https://www.interpol.int/fr/How-we-work/Notices/About-Notices.
[20] Étude approfondie de l'ONUDC sur la cybercriminalité, p.195.

Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité et le Groupe de travail à composition non limitée sur la sécurité du numérique[21].

Renforçant encore le partenariat entre les deux organisations, la résolution de l'Assemblée générale sur la coopération entre l'ONU et INTERPOL a été adopté à l'unanimité le 23 novembre 2020, à l'issue du deuxième examen biannuel de la résolution sur la question[22]. Ce texte est important car il a permis d'adopter de nouvelles dispositions dans des domaines clés de la coopération, notamment la cybercriminalité, de façon à renforcer la légitimité de l'approfondissement de la collaboration entre les deux organisations dans ce domaine.

À l'heure de la numérisation, les solutions nationales ou même régionales ne suffisent plus. Afin de contribuer à l'instauration de la paix et de la sécurité internationales dans le cyberespace, INTERPOL peut servir de mécanisme mondial permettant de lutter efficacement contre la cybercriminalité et de fournir à ses pays membres divers services et outils, à savoir notamment :

- Le système mondial de communication policière sécurisée I-24/7, qui permet de partager les informations policières urgentes en toute sécurité et en temps réel ;
- 19 bases de données[23] et notices[24] qui permettent de donner l'alerte au niveau international et de faciliter les enquêtes transnationales ;
- Le Programme mondial de lutte contre la cybercriminalité d'INTERPOL, qui s'appuie sur ses capacités policières en matière de prévention, de détection, d'enquête et de lutte contre la cybercriminalité pour réduire l'impact mondial de la cybercriminalité et protéger les populations, afin de rendre le monde plus sûr ;
- Le Groupe d'experts mondial d'INTERPOL sur la cybercriminalité et les groupes de travail régionaux composés de chefs de services de lutte contre la cybercriminalité, qui sont chargés d'examiner des questions de cybercriminalité urgentes et de concevoir des plans opérationnels et stratégiques ;
- Des plateformes de communication comme l'espace de travail Échange de connaissances sur la cybercriminalité, qui permet à l'ensemble des acteurs des services de maintien de l'ordre de partager des informations en toute sécurité, et la Plateforme collaborative sur la cybercriminalité – Opérations, qui permet l'échange confidentiel d'informations sur les questions opérationnelles ;
- La plateforme Cyber Fusion, qui sert à regrouper les données sur la cybercriminalité et à effectuer des analyses approfondies ;
- Le point de contact INTERPOL pour les questions de cybercriminalité, qui est joignable 24 heures sur 24 et 7 jours sur 7, permet de mettre en relation en temps réel les services de lutte contre la cybercriminalité de différents pays pour permettre la coopération ;
- La cellule de crise INTERPOL pour les cyberincidents (I-CIRT), qui permet de coordonner l'action des services de maintien de l'ordre du monde entier en cas de cyberincident majeur ;

---

[21] https://www.unodc.org/documents/Cybercrime/IEG_cyber_comments/INTERPOL.pdf et https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Statements/Item-3/INTERPOL_item_3.pdf.

[22] Résolution 75/10 de l'Assemblée générale sur la coopération entre l'Organisation des Nations Unies et l'Organisation internationale de police criminelle (INTERPOL).

[23] https://www.interpol.int/fr/How-we-work/Databases/Our-19-databases.

[24] https://www.interpol.int/fr/How-we-work/Notices/About-Notices.

- Le groupe de travail d'INTERPOL sur la criminalité financière mondiale, qui vise à réduire la criminalité financière et son impact à l'échelle mondiale en favorisant la coopération internationale et l'innovation, en mettant l'accent sur la cyberfraude et le blanchiment d'argent.

Approche multipartite

Les enquêtes sur la cybercriminalité présentent un certain nombre de difficultés à surmonter qui ne se posent pas dans le domaine physique. Pour les forces de l'ordre, il est difficile de déceler directement les attaques qui ont été commises ; de plus, les taux de signalement sont faibles. Les enquêtes sur les cas de cybercriminalité supposent également des compétences et des technologies particulières, qui ne sont pas disponibles partout. La cybercriminalité étant mondiale par nature, il est souvent difficile d'y faire face efficacement, dans les cas où les éléments de preuve et les suspects sont dispersés dans plusieurs juridictions.

Pour remédier à ces difficultés, INTEPROL a placé le partenariat au cœur de la lutte contre la cybercriminalité. À la quatre-vingt-huitième session de l'Assemblée générale d'INTERPOL, qui s'est tenue en 2019, les pays membres ont approuvé le cadre juridique « Gateway », qui permet à INTERPOL de partager des informations avec des entreprises du secteur privé[25]. Cette décision se fonde sur le fait que les services de maintien de l'ordre ont besoin de travailler en étroite collaboration avec le secteur privé, qui détient la majorité des données et des compétences en matière de cybercriminalité.

Le Programme mondial de lutte contre la cybercriminalité d'INTERPOL compte actuellement 12 partenaires dans le secteur privé, qui partagent des informations actualisées et des compétences en matière de cybercriminalité et apportent une assistance technique aux services de maintien de l'ordre. L'accès aux données – des secteurs public et privé – permet à INTERPOL de fournir à ses pays membres un soutien opérationnel et des conseils techniques en fonction de leurs besoins.

En outre, il est essentiel de collaborer avec divers acteurs de l'écosystème mondial de la cybersécurité, sachant que la disponibilité d'ensembles de données variés aide à élaborer des politiques efficaces et des interventions opérationnelles contre la cybercriminalité. Cela permet également de mettre en commun nos connaissances afin de pouvoir faire preuve de résilience et d'agilité en cette période d'incertitude. À la fin de l'année dernière, INTERPOL a aidé la police nigériane, conjointement avec un partenaire du secteur privé, à arrêter les membres d'un groupe criminel organisé qui était responsable de campagnes d'hameçonnage et d'escroqueries par compromission du courrier électronique d'entreprises qui ont touché des gouvernements et des entreprises privées dans plus de 150 pays[26].

INTERPOL met également l'accent sur la prévention. Pour prévenir la cybercriminalité, l'organisation travaille en étroite collaboration avec ses partenaires des secteurs public et privé pour promouvoir une bonne hygiène numérique grâce à une série de campagnes mondiales de sensibilisation. Ces efforts aident également les organismes chargés de l'application de la loi à surmonter les nombreuses difficultés rencontrées dans la lutte contre la cybercriminalité en sensibilisant le public aussi bien à cette forme de criminalité en soi, qu'aux moyens de s'en prémunir et d'y réagir.

---

[25] https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-s-General-Assembly-sets-road carte-pour-la-police-globale.

[26] https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/Arrestation-de-trois-personnes-INTERPOL-Group-IB-et-la-police-nigeriane-demantelent-un-groupe-de-cybermalfaiteurs-tres-actif.

Conclusion

Les rapports entre les criminels, les infrastructures ciblées et les victimes dépassent les frontières et les juridictions nationales, mais les services locaux de maintien de l'ordre n'ont pas toujours les capacités ou les moyens nécessaires pour s'attaquer à ces éléments transfrontières de la cybercriminalité. Les pays membres doivent garder à l'esprit que les lacunes de cybercapacités ou de capacités des services de maintien de l'ordre dans telle ou telle région constituent pour les réseaux criminels une opportunité clé, dont ils profitent pour situer leurs infrastructures et leurs activités là où le risque est moindre.

Pour atténuer les menaces et les risques en constante évolution qui sont associés au cyberespace, les pays membres devraient tirer le meilleur parti de la coopération policière pour agir avec rapidité et efficacité. Grâce à sa présence dans tous les pays, INTERPOL est en mesure de faire le lien entre les différents éléments afin d'identifier et de combattre les acteurs criminels dans le cyberespace, en collaboration avec ses pays membres et ses partenaires.

Il est évident que la cybercriminalité ne peut être combattue efficacement qu'au moyen d'une action qui soit coordonnée au niveau mondial et rapide, ce dernier point étant essentiel. Nous devons protéger les systèmes, préparer nos dirigeantes et dirigeants, partager les solutions et promouvoir les mesures nécessaires. En particulier, l'application de la loi doit se fonder sur des partenariats fiables et efficaces, l'échange de données étant essentiel, notamment entre les forces de police nationales, le secteur privé et les experts mondiaux tels qu'INTERPOL. Il est essentiel d'accroître la confiance au sein de la communauté mondiale des acteurs de l'application de la loi, grâce à une attitude qui consiste à « oser de partager », afin d'atteindre l'objectif commun de la lutte contre la cybercriminalité.

La communauté internationale est aujourd'hui soumise à une pression exceptionnelle. Pour assurer notre sécurité commune, il faut donc que nous accordions une place plus grande à la collaboration et l'inclusion. C'est la raison d'être d'INTERPOL : faciliter la coopération internationale entre les services de maintien de l'ordre pour bâtir un monde plus sûr. À cette fin, INTERPOL travaille aux côtés de l'ONU, étant convaincue que la sécurité et la justice sont essentielles à la mise en place d'un cyberespace pacifique et viable. Afin d'y parvenir, elle continuera d'aider ses pays membres à lutter contre la cybercriminalité.

Annexe XXXVIII

Déclaration du Représentant permanent de la République islamique d'Iran auprès de l'Organisation des Nations Unies, M. Majid Takht Ravanchi

Le cyberespace offre à l'humanité des opportunités inestimables pour développer et favoriser continuellement tous les aspects de la vie. Il faut donc non seulement promouvoir cet outil exceptionnel dans le monde entier, notamment dans les pays en développement, mais aussi le protéger contre toutes les menaces.

Le cyberespace peut aussi servir à commettre des actes d'agression et d'autres ruptures de la paix, à « recourir à la menace ou à l'emploi de la force », à « intervenir dans des affaires qui relèvent essentiellement de la compétence nationale d'un État », à violer la souveraineté des États ou à user de coercition contre d'autres États. Il faut s'attaquer efficacement à ces problèmes.

À titre général, les principes et normes applicables du droit international – bien entendu interprétés correctement et de façon non arbitraire – doivent régir les droits, les devoirs et les comportements des États dans le contexte du cyberespace.

Cependant, s'il n'existe pas de consensus sur l'applicabilité du droit international, ni même de normes internationales relatives au cyberespace, la communauté internationale doit s'efforcer d'élaborer les normes nécessaires.

À cette fin, étant donné qu'elle est chargée en vertu de la Charte du développement progressif du droit international et de sa codification, l'Assemblée générale doit poursuivre ses efforts pour élaborer et codifier les principes et normes internationaux nécessaires dans le domaine du cyberespace, y compris sous la forme d'un instrument international juridiquement contraignant.

Parallèlement à ces efforts, les États doivent s'efforcer de faire en sorte que le cyberespace soit utilisé aussi largement que possible dans l'optique de leur développement et, ce faisant, agir de manière responsable et conformément au droit international applicable et, en particulier, aux buts et principes des Nations Unies.

C'est à chaque État qu'il incombe au premier chef de faire en sorte que le cyberespace soit sûr, sécurisé et digne de confiance. Par conséquent, compte tenu de la complexité actuelle de la gouvernance du cyberespace, il convient de favoriser et de garantir des conditions qui donnent aux États un rôle actif et prépondérant dans la gouvernance de l'environnement du cyberespace au niveau mondial, notamment sur le plan des politiques et de la prise de décisions.

Dans le même temps, la gouvernance du cyberespace doit être planifiée de façon à ne pas porter atteinte aux droits des États en ce qui concerne leurs choix de développement, de gouvernance et de législation concernant l'environnement du cyberespace.

Il faut pleinement respecter le droit des États d'avoir « librement accès à l'information et de développer pleinement et sans ingérence leur système d'information et de communications et de mettre leurs moyens d'information au service de leurs aspirations et intérêts politiques, sociaux, économiques et culturels », ainsi que « le droit et le devoir des États de lutter, dans le cadre des prérogatives que leur confère leur constitution, contre la diffusion de nouvelles erronées ou déformées », qui a également été réaffirmé par l'Assemblée générale dans la Déclaration sur l'inadmissibilité de l'intervention et de l'ingérence dans les affaires intérieures des États de 1981.

Pour s'acquitter de la responsabilité qui leur incombe de garantir que le cyberespace soit sûr, sécurisé et fiable, les États doivent adopter une approche coopérative plutôt que conflictuelle.

Comme l'a réaffirmé l'Assemblée générale dans la Déclaration sur l'inadmissibilité de l'intervention dans les affaires intérieures des États et sur la protection de leur indépendance et de leur souveraineté de 1965, « Aucun État n'a le droit d'intervenir, directement ou indirectement, pour quelque raison que ce soit, dans les affaires intérieures ou extérieures d'un autre État ». Tous les États doivent donc prévenir les actes de ce type et s'en abstenir, notamment ceux qui visent des éléments politiques, économiques et culturels ou les infrastructures critiques des États liées au cyberespace, y compris par des moyens liés au cyberespace.

En outre, l'Assemblée, dans la Déclaration sur l'inadmissibilité de l'intervention et de l'ingérence dans les affaires intérieures des États de 1981, a réaffirmé le devoir qu'avait chaque État de « veiller à ce que son territoire ne soit pas utilisé d'une manière qui compromette la souveraineté, l'indépendance politique, l'intégrité territoriale et l'unité nationale ou perturbe la stabilité politique, économique et sociale d'un autre État », de « s'abstenir de toute action ou tentative, sous quelque forme ou quelque prétexte que ce soit, tendant à déstabiliser ou à compromettre la stabilité d'un autre État ou de l'une quelconque de ses institutions », de « s'abstenir de toute campagne de diffamation, de tout dénigrement ou propagande hostile aux fins d'intervention ou d'ingérence dans les affaires intérieures d'autres États ». Ces règles doivent également être respectées par les États dans le contexte du cyberespace.

Suivant l'un des principes réaffirmés par l'Assemblée générale dans la Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre les États conformément à la Charte des Nations Unies de 1970, les États ne doivent recourir à aucune mesure pour contraindre un autre État à lui subordonner l'exercice de ses droits souverains et pour en tirer un avantage quelconque. En conséquence, les États ne doivent pas exploiter les progrès accomplis dans le domaine du cyberespace pour prendre des mesures coercitives de nature économique, politique ou autre, y compris en limitant ou en empêchant l'application des mesures prises contre d'autres États.

De même, les États doivent s'abstenir de recourir à la menace ou à l'emploi de la force dans le cyberespace et au moyen de celui-ci. Ils doivent aussi empêcher que les chaînes d'approvisionnement numériques développées sous leur contrôle et leur juridiction soient utilisées pour créer ou contribuer à élaborer des produits, des services et une maintenance présentant des vulnérabilités de nature à compromettre la souveraineté et la protection des données d'autres États, et s'abstenir de l'utiliser à ces fins.

Les États doivent également exercer un contrôle adéquat sur les entreprises et les plateformes liées au cyberespace qui relèvent de leur juridiction, et prendre les mesures voulues pour qu'elles aient à répondre de leur comportement dans l'environnement numérique, notamment en cas d'atteinte à la souveraineté, à la sécurité et à l'ordre public d'autres États. En tout état de cause, les États sont responsables des actes internationalement illicites qu'ils commettent dans le cyberespace ou au moyen de celui-ci.

En outre, tous les différends internationaux liés au cyberespace doivent être réglés exclusivement par des moyens pacifiques, sur la base de l'égalité souveraine des États et conformément au principe du libre choix des moyens, comme indiqué dans la Déclaration de Manille sur le règlement pacifique des différends internationaux de 1970.

Il convient de rappeler à ce propos que, ces dernières années, nous avons été alarmés de voir certains États accuser systématiquement d'autres États d'avoir lancé des cyberattaques ou des activités similaires dans le cyberespace. Compte tenu des difficultés à surmonter en matière d'attribution des attaques dans le cyberespace ainsi que de l'absence d'un ensemble de normes élaborées et approuvées au niveau international en ce qui concerne les preuves authentiques, fiables et adéquates permettant d'étayer l'attribution, ces accusations ne peuvent être motivées que par des considérations d'ordre politique.

Dans l'ensemble, le cyberespace et les moyens, techniques et technologies qui y sont liés doivent servir exclusivement à des fins pacifiques et, pour atteindre cet objectif, les États doivent agir de manière coopérative, responsable et pleinement conforme au droit international applicable.

Enfin, nous adhérons au point de vue selon lequel il faut poursuivre l'examen des questions liées au cyberespace à l'Assemblée générale. Pour sa part, la République islamique d'Iran, qui fait partie des victimes de cyberattaques, ayant été visée par le ver informatique Stuxnet – lequel semble avoir été mis au point conjointement par les États-Unis et le régime israélien pour endommager les installations nucléaires pacifiques iraniennes – est prête à contribuer aux efforts que déploie l'Assemblée pour élaborer les principes et les normes nécessaires pour le cyberespace.

Annexe XXXIX

Déclaration de la Mission permanente auprès de l'Organisation des Nations Unies

L'Italie félicite l'Estonie d'avoir porté la question de la cybersécurité à l'attention du Conseil de sécurité et se réjouit de participer au débat public d'aujourd'hui.

Nous apprécions par ailleurs le soutien et le dévouement de la Haute-Représentante pour les affaires de désarmement, M^me^ Nakamitsu, qui a accepté de présenter un exposé de la situation au Conseil de sécurité à un moment où les États Membres sont préoccupés par la multiplication des incidents de cybersécurité.

L'Italie s'associe à la déclaration de l'Union européenne et souhaiterait ajouter les remarques suivantes à titre national.

Le présent débat ne pourrait avoir lieu à moment plus opportun. L'Assemblée générale a pris acte des travaux menés ces deux dernières années par la Première Commission sur les évolutions des technologies de l'information et des communications qui intéressent la sécurité internationale et sur les moyens de favoriser le comportement responsable des États dans le cyberespace. Les deux rapports adoptés par le Groupe de travail à composition non limitée et le Groupe d'experts gouvernementaux au cours du dernier semestre représentent des réalisations importantes qui devraient contribuer à renforcer la confiance entre les États Membres. Ils ont permis de faire mieux connaître un domaine qui, pendant plusieurs années, avait été considéré comme essentiellement technique.

La numérisation s'accélère au niveau mondial et, parallèlement aux avantages qui y sont associés, le défi consiste à faire en sorte que le cyberespace reste un domaine mondial, ouvert et stable. Il est déplorable de constater que les incidents se sont multipliés ces derniers mois, et que certains d'entre eux ont ciblé des infrastructures critiques et imposé des coûts élevés aux économies concernées. Certaines de ces attaques ont laissé entrevoir combien les actes de ce type risquent d'entraîner de pertes humaines, notamment dans le contexte d'une pandémie. Le potentiel destructeur de l'utilisation abusive des nouvelles technologies est de plus en plus manifeste, tout comme la nécessité de maintenir le contrôle sur ces technologies. L'Italie estime que c'est l'ONU qui est la mieux placée pour mener cette tâche à bien et pour promouvoir la paix et la stabilité dans le cyberespace.

L'Italie souhaite réaffirmer la position exprimée par l'Union européenne dans sa déclaration en qui concerne l'applicabilité du droit international au cyberespace, y compris le droit international humanitaire et les droits humains, l'importance du respect des normes relatives au comportement responsable des États et l'utilité des mesures de confiance comme moyen concret de prévenir les conflits. Elle souhaite également souligner le rôle important que peuvent jouer les organisations régionales dans le domaine de la cybersécurité. Fervente partisane du multilatéralisme, l'Italie encourage le dialogue entre l'ONU et les organisations régionales et se félicite à cet égard des récentes discussions entre le Secrétaire général de l'Organisation et le Conseil européen, qui représentent une occasion intéressante d'échanger des vues sur les problèmes auxquels nous sommes confrontés. Nous saluons également les efforts de la présidence suédoise de l'Organisation pour la sécurité et la coopération en Europe, qui s'emploie à mettre en évidence les liens entre droits humains, questions de genre et cybersécurité.

Dans un monde de plus en plus interconnecté, il devient encore plus nécessaire de dialoguer pour rapprocher les points de vue et accroître les possibilités de coopération. Dans cet esprit, nous appuyons le dialogue de l'Union européenne avec

l'ONU et les organisations régionales, notamment l'Union africaine, le Forum régional de l'Association des nations de l'Asie du Sud-Est et le Bureau du Conseiller spécial.

Par l'intermédiaire des organisations régionales, les États Membres peuvent optimiser leurs relations bilatérales, en mettant en commun les meilleures pratiques et les enseignements à retenir, et éviter ainsi que les approches régionales ne divergent les unes des autres. Il convient de consacrer plus d'efforts aux mécanismes de règlement pacifique des différends, ainsi qu'aux initiatives visant à développer la cyberdiplomatie et la cybermédiation.

Nous pensons que le cyberespace doit rester ouvert, libre, sûr et stable, car il constitue pour les États un moyen de mettre en œuvre des politiques qui permettront aux sociétés de s'épanouir et de garantir le développement durable pour tous, contribuant ainsi à la réalisation des objectifs de développement durable. Il ne faut pas sous-estimer l'importance du renforcement des capacités, qui garantit que la résilience des États soit homogène, fait mieux connaître les enjeux et stimule le développement des compétences. Il reste encore beaucoup à faire dans ce secteur, et nous pensons que le programme d'action visant à favoriser le comportement responsable des États dans le cyberespace, que nous soutenons avec 52 autres États Membres, pourrait être le mécanisme à exploiter en priorité pour coordonner et promouvoir l'action à mener. Nous nous sommes déjà déclarés prêts à poursuivre les échanges sur cette initiative dans le cadre des débats de la Première Commission et réaffirmons cette volonté aujourd'hui. Le programme d'action pourrait également servir de cadre à la conception de l'approche multipartite et à la création des partenariats public-privé.

La pandémie a été à l'origine d'un recul spectaculaire en 2020 et en 2021. Nos efforts communs doivent viser avant tout à relancer le développement durable, et le cyberespace est l'un des éléments essentiels à cette fin. L'Italie travaille à cet objectif en tant que membre du G7 et promeut cette vision dans le cadre de la présidence du G20 qu'elle assure actuellement. Le débat d'aujourd'hui constitue une étape clé en vue de faire mieux connaître la problématique, de garantir que la numérisation se déroule dans un cyberespace sûr et stable, et de préserver tous les efforts accomplis.

Au moment où nous tenons ce débat, les ministres des affaires étrangères du G20 sont réunis à Matera pour discuter de questions de relance et de développement durable, l'objectif étant de ne laisser personne de côté. Nous espérons que ces efforts se renforceront mutuellement et que le Conseil de sécurité continuera de prêter attention aux questions liées au cyberespace et de suivre les progrès accomplis et qu'il rappellera leurs obligations aux États qui ne les respectent pas. Il faut espérer que ces cas seront très rares, sachant que les États Membres sont de plus en plus d'accord sur la nécessité de consacrer du temps et des efforts à un programme de cybersécurité qui soit constructif et qui renforce la confiance, la transparence et l'inclusion.

Annexe XL

Déclaration de l'Ambassadeur pour les affaires des Nations Unies et la cyberpolitique du Ministère japonais des affaires étrangères, Akahori Takeshi

Le Japon tient à remercier sincèrement Kaja Kallas, Première Ministre de la République d'Estonie, d'avoir organisé ce débat public sur la cybersécurité. Le Japon remercie également l'Estonie d'avoir rappelé dans sa note de cadrage le débat public sur problèmes contemporains complexes pesant sur la paix et la sécurité internationales, qui avait été organisé en 2017 sous la présidence du Japon.

Le Japon se félicite de l'adoption du rapport du Groupe de travail à composition non limitée en mars et de l'adoption du rapport du sixième Groupe d'experts gouvernementaux en mai, par consensus dans les deux cas.

Le rapport du Groupe de travail à composition non limitée a ceci de précieux qu'il a été adopté par consensus à l'issue d'un processus auquel tous les États Membres ont pu pleinement participer. Les États membres y ont affirmé explicitement les acquis, à savoir que le droit international, en particulier la Charte des Nations Unies, était intégralement applicable au cyberespace.

Le rapport du Groupe d'experts gouvernementaux présente sa propre valeur ajoutée. Pour chacune des 11 normes figurant dans son rapport de 2015, le Groupe d'experts donne des indications et des exemples de mise en œuvre. Le Japon espère que cela favorisera la coopération internationale en vue de promouvoir le comportement responsable des États. En outre, il est désormais mieux établi que les faits internationalement illicites attribuables à un État engagent la responsabilité de ce dernier. L'applicabilité du droit international humanitaire est affirmée clairement dans le rapport. Le Groupe a de nouveau rappelé que les États avaient le droit inaliénable de prendre les mesures prévues dans la Charte.

Nous nous réjouissons à la perspective d'approfondir, dans divers lieux et contextes, les discussions concrètes sur l'application du droit international au cyberespace. Le Japon espère que le document de position qu'il a soumis au Groupe d'experts gouvernementaux pour qu'il l'intègre dans son recueil des positions nationales contribuera à ces débats. Je souhaiterais exposer aujourd'hui les principaux points de la position du Japon.

Le Japon estime que les États doivent s'abstenir de violer la souveraineté des autres États dans le cadre de leur cyberopérations. En outre, ils ne doivent pas intervenir dans les affaires relevant de la compétence nationale d'autres État en menant des cyberopérations. Les actes contraires au droit international qu'un État commet dans le cyberespace engagent sa responsabilité.

Ce droit impose aux États un devoir de précaution en la matière. Les normes 13 c) et f) et la deuxième phrase du paragraphe 71 g) du rapport du Groupe d'experts gouvernementaux de 2021 ont trait à ce devoir. En ce qui concerne l'attaque subie récemment par l'entreprise Colonial Pipeline, le Président des États-Unis a mentionné l'action menée pour établir « une sorte de norme internationale imposant aux gouvernements qui savent que des activités criminelles sont menées à partir de leur territoire de réagir à ces activités ». Nous reconnaissons qu'il est difficile d'attribuer des cyberopérations à tel ou tel État. Le devoir de précaution peut permettre d'engager la responsabilité de l'État lorsqu'une cyberopération qui ne serait autrement pas attribuable à un État a été lancée à partir de son territoire.

Tout différend international ayant trait à des cyberopérations doit être réglé par des moyens pacifiques conformément au paragraphe 3 de l'Article 2 de la Charte des

Nations Unies. Afin de garantir le règlement pacifique des différends qui résultent de cyberopérations, il convient de recourir aux pouvoirs qui sont conférés au Conseil de sécurité en vertu des chapitres VI et VII de la Charte ainsi qu'aux fonctions dont sont investies les autres organes de l'ONU. Le Japon a des réserves quant à l'idée d'établir un nouveau mécanisme international pour l'attribution des activités en question.

Si une cyberopération constitue une agression armée au sens de l'Article 51 de la Charte des Nations Unies, les États peuvent exercer leur droit inaliénable à la légitime défense, individuelle ou collective, qui leur est reconnu en vertu du même article.

Le droit international humanitaire est applicable aux cyberopérations. Ce principe contribue à la réglementation des méthodes et moyens de guerre. L'argument selon lequel il conduirait à la militarisation du cyberespace est sans fondement.

Le droit international des droits humains est lui aussi applicable aux cyberopérations. Le contexte des cyberopérations ne modifie pas les droits humains dont bénéficie chacune et chacun.

En ce qui concerne les rapports entre droit international et normes internationales facultatives, dans la perspective de la stabilisation du cyberespace, il est essentiel que ces domaines contribuent tous deux à prévenir les actes internationalement illicites impliquant des TIC et à promouvoir le comportement responsable des États dans le cyberespace. Comme l'exprime clairement le rapport du Groupe de travail à composition non limitée, ces normes ne remplacent pas ni ne modifient les obligations que le droit international impose aux États.

Le Japon espère qu'un grand nombre d'États Membres présenteront à titre volontaire leur position sur l'application du droit international.

Le Japon estime qu'il est temps de donner la priorité à l'application des obligations et des normes facultatives qui ont été adoptées dans le cadre du droit international, ainsi qu'aux mesures de confiance et de renforcement des capacités.

Dans le cadre de leur application, le Japon souhaiterait inviter les États à faire connaître sans attendre leur évaluation juridique des cyberopérations malveillantes lorsqu'elles se produisent, notamment en ce qui concerne la question de savoir si l'opération en question constitue une violation du droit international. Cela contribuerait à faire naître une conception commune de l'application du droit international aux cyberopérations. L'application aux cyberincidents du droit international par les cours et tribunaux internationaux irait dans le même sens. Le Japon espère que ces pratiques concourront à décourager les activités malveillantes dans le cyberespace.

Le Japon soutient fermement le programme d'action. Nous pensons que le programme d'action contribuera efficacement à garantir et à suivre l'application des normes convenues, des obligations découlant du droit international et des mesures de confiance et de renforcement des capacités. Nous nous réjouissons à la perspective d'approfondir les discussions sur le programme d'action. Nous continuerons également de participer activement aux travaux du nouveau Groupe de travail à composition non limitée.

Le Japon est résolu à œuvrer pour que le cyberespace reste libre, équitable et sûr et à contribuer activement aux discussions et aux efforts visant à promouvoir l'état de droit dans le cyberespace, notamment à l'ONU.

Annexe XLI

Déclaration du Représentant permanent du Kazakhstan auprès de l'Organisation des Nations Unies, M. Magzhan Ilyassov

Nous savons gré à l'Estonie, qui assure la présidence, d'avoir organisé et dirigé le débat sur le thème « **Maintien de la paix et de la sécurité internationales : cybersécurité** ».

Face aux menaces mondiales, le maintien de la sécurité passe par l'action coordonnée de la communauté internationale et le règlement d'une série de questions politiques et économiques. Dans ce contexte, il faut prendre acte de l'apparition d'une question nouvelle et complexe : la cybersécurité.

À l'évidence, les technologies de l'information et des communications (TIC) ont un potentiel énorme pour le développement des États. Dans le même temps, elles offrent de nouvelles possibilités aux criminels et pourraient faire croître le nombre et la complexité des actes illicites, et les technologies émergentes, notamment l'intelligence artificielle, risquent d'être utilisées de façon abusive. À cet égard, la prévention et l'élimination de l'utilisation criminelle des TIC devraient figurer aujourd'hui parmi les priorités de l'action publique.

À cet égard, nous nous félicitons de la création d'un groupe d'experts intergouvernemental à composition non limitée, représentant toutes les régions et chargé d'élaborer un instrument international complet sur la lutte contre l'utilisation des TIC à des fins criminelles, en tenant pleinement compte des instruments internationaux existants et des efforts déployés aux niveaux national, régional et international contre l'utilisation des technologies de l'information et des communications à des fins criminelles, comme prévu dans la résolution 74/247 adoptée par l'Assemblée générale le 27 décembre 2019.

Nous pensons que les travaux de l'ONU dans ce domaine seront éclairés par le rapport final du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, adopté en mars 2021, et par le consensus exprimé dans la résolution 75/240, dans laquelle l'Assemblée générale a créé le Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), ainsi que par le rapport adopté par consensus en mai 2021 par le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale.

Les États devraient continuer à renforcer les mesures visant à protéger toutes les infrastructures critiques contre les menaces liées aux TIC et multiplier les échanges concernant les bonnes pratiques dans ce domaine.

À cet égard, nous nous félicitons du processus de négociation sur la cybersécurité qui est en cours à l'ONU et du fait que les participants et les États Membres s'entendent à penser que les décisions sur cette question doivent être prises par consensus.

Annexe XLII

Déclaration de la Mission permanente de la Lettonie auprès de l'Organisation des Nations Unies

Les développements des technologies de l'information et des communications (TIC) ont apporté aux États et aux sociétés une myriade d'avantages dans les domaines de l'économie, des services, de l'éducation et de la communication. Sans oublier les effets largement positifs des applications des TIC, la Lettonie est de plus en plus préoccupée par les effets des utilisations malveillantes et perturbatrices de ces technologies, ainsi que de leurs conséquences pour la paix, la sécurité et la stabilité internationales et pour les droits humains.

Il est devenu plus fréquent que les États soient victimes de ces infractions, notamment celles qui visent des institutions démocratiques et des infrastructures critiques. Il est encore plus alarmant que des acteurs qui mènent des cyberactivités malveillantes profitent de la pandémie de coronavirus en ciblant les systèmes médicaux essentiels au maintien de la santé humaine, les activités de recherche de vaccins ainsi que le domaine de l'information.

La large participation à la réunion organisée par le Conseil de sécurité selon la formule Arria l'année dernière et les débats qui y ont été tenus ont confirmé que la cybersécurité revêtait une importance de plus en plus grande pour la paix et la stabilité internationales. Il est tout à fait pertinent et opportun d'inscrire la question de la cybersécurité au programme de travail officiel du Conseil. La Lettonie soutient sans réserve les efforts que déploie l'Estonie pour bien examiner les moyens d'atténuer l'impact des comportements irresponsables dans le cyberespace sur la paix et la sécurité internationales.

L'ONU doit continuer de jouer un rôle important au niveau international pour promouvoir la paix, la sécurité et la stabilité, y compris dans le cyberespace. Par les travaux qu'ils se sont employés à mener, le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale ont beaucoup contribué à préparer les débats de la présente réunion.

L'adoption par consensus du rapport final du Groupe d'experts gouvernementaux et de celui du Groupe de travail à composition non limitée représente une étape utile dans l'action qu'il faut continuer de mener pour parvenir à une conception commune de toute une série de questions.

À cet égard, le programme d'action en faveur de l'utilisation responsable des TIC par les États dans le contexte de la sécurité internationale est un résultat précieux des rapports de ces deux groupes. Ce programme d'action, dont la principale qualité est d'être axé sur les mesures concrètes, fournira une base solide à l'action à la poursuite des travaux visant à faire avancer concrètement l'application des normes relatives au comportement responsable.

Dans ce contexte, la Lettonie tient à souligner que les débats sur le cyberespace doivent être multipartites, comme ils nécessitent la participation d'une série d'acteurs non étatiques issus du secteur privé, de la société civile et du monde de la recherche. Compte tenu de leurs rôles majeurs dans l'écosystème des TIC, ces parties prenantes peuvent contribuer à apporter aux travaux des contributions diverses et nombreuses, en partageant leurs points de vue, leurs connaissances et leur expérience.

Les États devraient continuer de s'employer activement à promouvoir le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et, à cette fin, se ternir prêts à avoir des échanges approfondis dans le cadre des processus qui seront menés à l'ONU. Nous devons tous nous employer sans relâche à renforcer la protection et la sécurité de nos propres TIC, mais il faut aussi que les États empêchent les autres États et les acteurs non étatiques d'utiliser des TIC à partir de leur territoire pour commettre des actes internationalement illicites. Nous appelons tous les États à s'abstenir de mener, de permettre ou de tolérer de telles activités, qui sont contraires au droit international et notamment à la Charte des Nations Unies, afin d'éviter de compromettre la sécurité de l'utilisation des TIC. La responsabilité, la confiance et la prévisibilité doivent être au centre de la coopération internationale dans le domaine de la cybersécurité.

Afin d'éviter les malentendus et les perceptions erronées, d'une part, et d'établir une pratique en ce qui concerne la communication d'informations sur les incidents liés aux TIC, d'autre part, nous devons mettre en place des voies de communication entre les États Membres. La création d'un réseau de points de contact aux niveaux politique et technique à l'ONU est susceptible de contribuer considérablement à améliorer la communication à l'échelon mondial. L'efficacité d'une telle démarche a déjà été démontrée au niveau régional, à l'Organisation pour la sécurité et la coopération en Europe.

Enfin, la Lettonie souhaite féliciter tous les États Membres d'avoir fait preuve de leur volonté de coopérer et de travailler ensemble pour parvenir à un consensus sur les rapports du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée. Ils se sont ainsi engagés sur la bonne voie et ont créé une excellente occasion de renforcer encore la coopération internationale nécessaire à la mise en place d'un cyberespace mondial qui soit ouvert, stable, pacifique et sûr, et dans lequel les droits humains, les libertés fondamentales et l'état de droit sont pleinement appliqués.

Annexe XLIII

Déclaration du Chargé d'affaires par intérim et Représentant permanent adjoint du Liechtenstein auprès de l'Organisation des Nations Unies, Georg Sparber

Les cyberopérations ont joué un rôle d'égalisation dans le contexte des guerres modernes, ayant créé de nouvelles possibilités d'opérations offensives et défensives pour tous les acteurs, y compris ceux qui disposent de moins de ressources. En conséquence, les cyberattaques sont devenues plus fréquentes et plus destructives ces dernières années et compromettent maintenant la paix et la sécurité internationales. Il est alarmant de constater que ces attaques sont susceptibles de causer de graves souffrances à la population civile, notamment la perte de vies humaines et l'interruption de services essentiels. Dans ce contexte, nous rappelons que les États adhèrent de plus en plus au principe selon lequel le droit international s'applique au cyberespace, s'agissant notamment de la Charte des Nations Unies dans son intégralité et des règles du droit international coutumier qui découlent des principes énoncés dans la Charte, ainsi que du Statut de Rome de la Cour pénale internationale et du droit international humanitaire.

Le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale a institutionnalisé les débats sur la paix et la sécurité internationales et le cyberespace au sein de l'ONU. En outre, dans son rapport final, 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 (Groupe d'experts gouvernementaux) réaffirme l'applicabilité et la nécessité du droit international dans le cyberespace. Le Liechtenstein prend note des contributions faites par le Groupe de travail à composition non limitée et le Groupe d'experts gouvernementaux pour faire avancer le débat sur les modalités de l'application au cyberespace du droit international, en particulier de la Charte des Nations Unies.

L'un des progrès décisifs accomplis grâce à la Charte réside dans l'interdiction de l'emploi de la force. La Charte interdit en effet le recours à la force, sauf s'il est autorisé par le Conseil de sécurité en vertu du chapitre VII ou s'il est relève de la légitime défense au sens de l'Article 51. Cependant, l'Article 51 est de plus en plus souvent invoqué pour justifier le recours à la force en l'absence des fondements juridiques nécessaires. Cette tendance risque fort de s'étendre au cyberespace à mesure que se développent les nouvelles technologies et les capacités des États. Nous devons veiller à ce que le cyberespace ne facilite pas des actes injustifiés au nom de la légitime défense. Et nous rappelons que pour pouvoir invoquer l'Article 51 à titre préventif, il faut faire la preuve de l'imminence d'une attaque armée, ainsi que de la nécessité et de la proportionnalité des mesures qui sont prises.

En vertu de la Charte des Nations Unies, le Conseil de sécurité à un rôle à jouer pour faire respecter les règles applicables du droit international dans le cas des violations graves qui constituent des actes d'agression. Outre les outils prévus dans la Charte, le Conseil a maintenant la possibilité d'engager la responsabilité pénale individuelle des auteurs d'un acte d'agression en saisissant la Cour pénale internationale. Dans ce contexte, le Liechtenstein estime que les travaux du Conseil bénéficieraient d'une conception claire de l'application du Statut de Rome aux cyberopérations.

Afin de mieux comprendre l'application du Statut de Rome aux cyberopérations, le Liechtenstein et dix autres États membres de la CPI ont créé un conseil consultatif

chargé d'étudier l'application du Statut de Rome à la réglementation des cyberguerres. Composé de 16 éminents juristes internationaux, le conseil consultatif s'est réuni trois fois au cours des années 2019 et 2020 pour examiner dans quelle mesure les dispositions fondamentales du Statut de Rome s'appliquaient aux cyberopérations. Il devrait présenter son rapport final cette année. Nous espérons que ces travaux contribueront à faire émerger une conception commune de la responsabilité dans le contexte des cyberopérations, ainsi que des moyens de prévenir les crimes en question avant qu'ils ne se produisent.

Le Liechtenstein souligne que nous avons besoin d'un cadre juridique solide pour réglementer le cyberespace afin de garantir la paix et la sécurité internationales. Nous nous réjouissons à la perspective de contribuer à la lutte mondiale contre les cyberopérations malveillantes en publiant prochainement un rapport sur le Statut de Rome, et nous continuerons d'œuvrer en faveur de la paix et de la sécurité internationales conformément à notre attachement inébranlable au droit international.

Annexe XLIV

Déclaration de la Mission permanente de Malte auprès de l'Organisation des Nations Unies

Malte remercie l'Estonie d'avoir organisé ce débat, qui arrive à point nommé, sur une question dont elle estime que le Conseil devrait être saisi. Les questions liées à la cybersécurité ont certes été évoquées à l'occasion de plusieurs débats du Conseil, mais Malte est d'avis qu'on devrait leur accorder davantage de place encore, puisqu'elles sont parmi les problèmes les plus graves et les plus évolutifs qui pèsent sur la paix et la sécurité internationale.

Malte s'associe à la déclaration faite par l'Union européenne et voudrait appeler l'attention sur quelques points à titre national. Le développement du cyberespace a offert de nouvelles perspectives aux États Membres et aux citoyennes et citoyens du monde entier. Il a été un facteur de prospérité, de connectivité et de croissance économique. Cependant, il a aussi ouvert la voie à des activités malveillantes visant à perturber les sociétés, à en exploiter les faiblesses et à lancer des attaques pouvant nuire gravement aux États Membres et à leur population, par exemple dans les domaines des données sensibles et des infrastructures critiques. De fait, le monde virtuel et interconnecté occupe de plus en plus de place dans nos vies, ce qui nous rend de plus en plus vulnérable à ce type d'activités.

Malte estime que l'ONU a un rôle central à jouer dans la réglementation du comportement des États dans le cyberespace, tout particulièrement compte tenu du vaste corpus de droit international existant. Elle a trouvé très encourageants les résultats obtenus par le Groupe d'experts gouvernementaux et le Groupe de travail à composition non limitée, qui ont adopté des rapports de consensus portant notamment sur les moyens de favoriser le comportement responsable des États dans le cyberespace. Il est indispensable de poursuivre ces processus pour nourrir les travaux du système des Nations Unies et préciser la manière dont le droit international s'applique au cyberespace, rappeler l'importance des mesures de confiance et produire de nouvelles normes et directives. Nous savons combien la participation et la contribution des États Membres à ces processus sont précieuses et souhaitons vivement que les discussions avancent en suivant le rythme rapide auquel le sujet évolue.

On sait que les cyberattaques peuvent avoir des effets dévastateurs sur les données sensibles et les infrastructures. Il est vital de définir clairement des normes et des règles régissant le comportement des États dans le cyberespace. On pourra ainsi mieux anticiper les cybermenaces et éviter toute erreur dans leur appréciation. Le potentiel de nuisance à long terme des utilisations malveillantes du cyberespace est tel qu'il faut également coopérer au niveau international afin d'éviter les conflits auxquels elles pourraient donner lieu.

Les mesures visant à renforcer la confiance entre les États, au moyen de bonnes pratiques et de normes établies, seront pour l'avenir des outils essentiels, qui permettront de limiter tout risque de malentendu et de mieux évaluer les comportements malveillants.

La communauté internationale doit par ailleurs se rapprocher de la multitude d'autres parties prenantes concernées, dont la société civile et le secteur privé, dans un souci d'égalité des chances et afin d'établir un ensemble de règles équitables. Tous les utilisateurs et utilisatrices potentiels du cyberespace doivent prendre conscience qu'ils sont acteurs du renforcement de la cyberrésilience comme de la prévention de l'utilisation malveillante des outils dont ils disposent.

Malte estime que le Conseil de sécurité a un rôle important à jouer en ce qui concerne les nouvelles technologies qui pourraient avoir des incidences sur la paix et la sécurité internationales. Le Conseil doit veiller à ce que toutes les parties prenantes dans le cyberespace respectent le droit international et les règles et directives établies, afin d'éviter les conflits auxquels des cyberattaques pourraient donner lieu. Nous l'exhortons à rester saisi de la question et à faire en sorte qu'ensemble, nous favorisions la compréhension et la confiance réciproque.

Annexe XLV

Déclaration de la Mission permanente du Maroc auprès de l'Organisation des Nations Unies

[Original : français]

Le Royaume du Maroc remercie, tout d'abord, l'Estonie pour l'organisation de ce premier débat ouvert du Conseil de sécurité, consacré à la question, autant pertinente qu'opportune, du maintien de la paix et de la sécurité internationales dans le cyberespace. Le Maroc salue l'intervention exhaustive de M^me^ Kaja Kallas, Première Ministre de la République d'Estonie, ainsi que l'excellent leadership de l'Estonie sur les questions cybernétiques et de la sécurité du cyberespace. Le Maroc remercie, également, la Haute-Représentante pour les affaires de désarmement, M^me^ Izumi Nakamitsu, pour son exposé informatif sur les défis actuels au maintien de la paix et de la sécurité internationales dans le cyberespace.

En tant que pays en développement «hautement connecté», le Royaume du Maroc a, très tôt, attaché un intérêt particulier au développement des technologies de l'information et des communications (TIC), et à leurs atouts en tant que moteurs de développement durable. Toutefois, bien qu'il existe une unanimité sur les bienfaits et avantages apportés par les progrès des TIC au bien-être quotidien de l'humanité, une prise de conscience globale a commencé à s'installer quant aux menaces qui peuvent en émaner, allant de la simple circulation d'infox, aux réelles atteintes à la paix et à la sécurité, tant à l'échelle nationale qu'internationale.

À l'heure où l'on parle de termes assumés d'Internet des objets, de révolution digitale ou de cyberguerre, notre aptitude à combattre les menaces cybernétiques est, toutefois, restée en-deçà de notre haut niveau de dépendance à ces outils incontournables. De surcroît, il est important de constater que le contexte actuel marqué par la pandémie de la maladie à coronavirus (COVID-19) nous a, non seulement, davantage propulsé dans l'ère cybernétique, mais nous a, parallèlement, exposé à un niveau, exponentiel et irréversible, de vulnérabilités aux cyberattaques et menaces, y compris celles ciblant les infrastructures critiques.

De telles opérations malveillantes, au-delà de menacer la souveraineté des États, ont le regrettable potentiel d'augmenter le risque de conflits dans le cyberespace mais aussi de causer des dommages humains et matériels considérables. Ce qui est de nature à miner l'édifice de la paix et de la sécurité internationales et ériger les cyberattaques comme une menace émergente majeure.

«Nous vivons dans une époque dangereuse» comme l'a affirmé le Secrétaire général, lors du lancement de son programme de désarmement en 2018.

En effet, les risques potentiels et réels liés aux menaces dans le cyberspace interpellent, aujourd'hui plus que jamais, la communauté internationale et les États Membres de l'ONU. Ce n'est qu'en s'efforçant, collectivement et individuellement, de prévenir les usages malveillants des TIC que nous pourrons garantir que le cyberespace continuera à servir de moteur de paix, de sécurité, de stabilité et de développement.

À cet égard, le Maroc estime que le besoin de sécuriser et de protéger le cyberespace reste une responsabilité partagée des États, premiers chefs de file. C'est pourquoi le Maroc a, conformément aux Hautes Orientations Royales, entrepris, dès la première heure, d'importantes actions sur les plans législatif, organisationnel et préventif, dont :

- La déclinaison d'une stratégie de cybersécurité, s'articulant autour des quatre axes stratégiques de : l'évaluation des risques pesant sur les systèmes

d'information au sein des administrations, organismes publics et infrastructures d'importance vitale ; la protection et la défense de ces systèmes d'information ; le renforcement des fondements de la sécurité (cadre juridique, sensibilisation, formation et recherche et développement) ; et la promotion et le développement de la coopération nationale régionale et internationale ;

- La promulgation, le 25 juillet 2020, de la Loi n°05-20 relative à la cybersécurité, qui vise la mise en place d'un cadre juridique préconisant aux entités un socle minimal de règles et de mesures de sécurité, afin d'assurer la fiabilité et la résilience de leurs systèmes d'information. Elle a aussi pour objectifs le développement de la confiance numérique, la digitalisation de l'économie et, plus généralement, l'assurance de la continuité des activités économiques et sociétales du Maroc et ce, afin de favoriser le développement d'un écosystème national de cybersécurité ;

- La création, au cours de cette décennie, de plusieurs organisations visant à assurer la gouvernance étatique de la cybersécurité, telles que le Comité stratégique de la sécurité des systèmes d'information en 2011, la Direction générale de la sécurité des systèmes d'information, l'Agence nationale de réglementation des télécommunications, la Commission nationale de contrôle de la protection des données à caractère personnel ou encore le Centre marocain de recherches polytechniques et d'innovation qui porte la campagne nationale de lutte contre la cybercriminalité.

À la veille de la tenue de ce débat public, le Maroc a également approuvé, le 28 juin 2021, un projet de décret ayant trait à la cybersécurité qui fixe les règles applicables en matière de sécurité des systèmes d'information, ainsi que la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel.

Toutefois, au vu de la nature globale des menaces cybernétiques, d'importantes mesures internationalement agréées doivent pouvoir agir en complément des réglementions mises en œuvre sur le plan national. C'est pourquoi le Maroc a ratifié la Convention sur la cybercriminalité du Conseil de l'Europe, également connue sous le nom de Convention de Budapest, et en 2018, a joint l'Appel de Paris pour la confiance et la sécurité dans le cyberespace. Il participe, dans le cadre des Nations Unies, au Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, au Groupe d'experts gouvernementaux pour favoriser un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, au nouveau Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et à l'élaboration du prochain programme d'action pour favoriser un comportement responsable des États dans le cyberespace. Le Maroc est, également, membre du Groupe des amis sur la gouvernance électronique et la cybersécurité que l'Estonie copréside, excellemment, aux côtés de Singapour.

Pour conclure, le Royaume du Maroc souligne qu'il est de la responsabilité partagée des États de faire preuve d'une volonté commune et ferme pour protéger le cyberespace et ce, principalement du fait que les volets de la prévention et de la sécurité du cyberespace sont des corollaires de l'usage des TIC.

En particulier, le Conseil de sécurité est appelé à jouer un rôle clef, notamment lorsque la survenue de cyberattaques constitue une menace directe pour la paix et la sécurité internationales, mais aussi pionnier en matière de prévention.

Le Maroc réitère ses vifs remerciements à l'Estonie pour avoir organisé un tel débat ouvert, nécessaire et opportun, car nous avons besoin d'une plus grande

sensibilisation et de discussions sur la question du maintien de la paix et de la sécurité internationales dans le cyberespace et pour avoir introduit cette question dans l'agenda du Conseil de sécurité.

Annexe XLVI

Déclaration de la Représentante permanente des Pays-Bas auprès de l'Organisation des Nations Unies, M^me^ Yoka Brandt

Le Royaume des Pays-Bas tient à remercier l'Estonie et sa Première Ministre, M^me^ Kallas, d'avoir organisé ce débat public sur le maintien de la paix et la sécurité internationales dans le cyberespace.

Cette réunion est fort opportune, compte tenu de la multiplication des cyberattaques conduites aussi bien par des États que par des acteurs non étatiques. Alors mêmes qu'elles ne mobilisent que relativement peu de moyens, les cyberactivités malveillantes peuvent perturber profondément nos sociétés, et déstabiliser les relations internationales.

Le moment est donc venu d'œuvrer ensemble pour faire du cyberespace un lieu ouvert, libre et sûr, en favorisant un comportement responsable des États, en dénonçant tout agissement irresponsable et en y opposant des conséquences.

Tout en sachant que la question peut être abordée sous de très nombreux angles pertinents, les Pays-Bas se borneront à évoquer trois éléments incontournables du renforcement de la stabilité dans le cyberespace :

- Préservation des acquis ;
- Attribution ;
- Renforcement des capacités.

Préservation des acquis

Au fil des ans, les cyberopérations contre des infrastructures critiques et civiles sont clairement devenues une menace réelle et crédible. On l'a encore constaté cette année, qui a été marquée par des cyberattaques d'une portée, d'une ampleur, d'une gravité et d'une sophistication nouvelles. Nos sociétés se sont progressivement tournées vers le numérique dans quasi tous les aspects de la vie ; nous devons comprendre que c'est par Internet que passent nos connections d'un bout à l'autre de la planète. Il n'est donc pas surprenant que les effets néfastes de cyberopérations malveillantes lancées contre des infrastructures critiques, des gouvernements ou des sociétés se fassent ressentir immédiatement et à grande échelle, compromettant grandement la sécurité et la stabilité internationales, le développement économique et social ainsi que la sécurité et le bien-être individuels.

Un consensus ayant été trouvé récemment concernant les rapports du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, les États disposent à présent d'un cadre régissant le comportement responsable des États dans le cyberespace qui leur permet de mieux comprendre la manière dont s'y appliquent le droit international et les 11 normes volontaires non contraignantes convenues. Les Pays-Bas rappellent que le droit international en vigueur, et en particulier la Charte des Nations Unies, sont applicables au cyberespace et qu'il est essentiel de les observer pour maintenir la paix et la stabilité et promouvoir un cyberespace libre, ouvert et sûr, où prévale notamment le respect des droits humains et des libertés fondamentales.

Les États sont convenus de bannir les cyberopérations contre des infrastructures et infrastructures d'information essentielles à la fournitures de services au public,

conformément à la norme 13 f) établie par le Groupe d'experts gouvernementaux. Il appartient à chaque État de déterminer les infrastructures qu'il considère comme critiques, mais cette catégorie peut recouvrir, par exemple, les établissements médicaux, les services financiers et des infrastructures liées à l'énergie, à l'eau, aux transports et à l'assainissement. Les Pays-Bas accordent de longue date une attention particulière à trois types d'infrastructures, à savoir :

1. Les infrastructures techniques essentielles à la disponibilité générale ou à l'intégrité d'Internet ;

Les infrastructures techniques nécessaires aux processus électoraux ;

Les infrastructures de santé.

Dans cet esprit, nous engageons les États à détailler les catégories d'infrastructures qu'ils considèrent comme essentielles et à les faire connaître publiquement en publiant des déclarations nationales et en précisant leur position vis-à-vis du cadre relatif au comportement responsable des États. C'est là le seul moyen d'améliorer la transparence, de parvenir à une vision commune, d'accroître la prévisibilité et de renforcer la confiance. Pour limiter le risque d'escalade, il faut poursuivre l'action menée à l'appui de la mise en œuvre du cadre convenu et veiller à ce que les États se tiennent aux acquis déjà constitués.

Attribution

Il existe un consensus apparent en ce qui concerne les règles et normes applicables dans le cyberespace. Pourtant, les cybermenaces ne cessent de se multiplier. Les Pays-Bas est consterné par le fait que la pandémie de maladie à coronavirus (COVID-19) ait été exploitée comme une occasion de lancer des cyberattaques malveillantes contre des infrastructures critiques, le secteur de la santé, les infrastructures techniques essentielles à la disponibilité générale ou à l'intégrité d'Internet et aux processus électoraux.

Soyons clairs – nous œuvrerons collectivement, sur une base volontaire, pour faire en sorte que les États qui ne se conforment pas au cadre rendent des comptes. Cela passera notamment par la mise en œuvre de mesures transparentes et conformes au droit international. Les comportements répréhensibles dans le cyberespace ne doivent pas rester impunis.

Renforcement des capacités

C'est par la résilience numérique que l'on parviendra à gérer les risques cybernétiques et à atténuer leurs impacts. Cependant, les capacités en matière de cybersécurité varient d'un État à l'autre, ce qui nous rend tous vulnérables dans un monde interconnecté. Il est donc dans notre intérêt commun de lancer des efforts de renforcement des capacités ciblées afin que tous les États responsables puissent appliquer le cadre et mieux protéger leurs réseaux face aux cyberactivités d'ampleur et à leur potentiel de perturbation, de destruction ou de déstabilisation. Pour que cet effort de renforcement des cybercapacités soit efficace, il faut que les États et les acteurs non étatiques coopèrent. C'est dans cette optique que les Pays-Bas ont créé le Forum mondial sur la cyber expertise, qui a évolué en une plateforme robuste de renforcement des capacités publiques et privées soutenant et regroupant les plus de 700 initiatives en cours visant à contribuer à renforcer la résilience technique en matière cybernétique et à élaborer des textes de loi propres à faire du cyberespace un espace sûr et sécurisé où les droits humains sont respectés.

Nous félicitons l’Estonie d’avoir posé les bases de futures discussions sur la cybersécurité au Conseil de sécurité et accueillons avec satisfaction le premier débat officiel tenu aujourd’hui sur la question.

Annexe XLVII

Déclaration de la Mission permanente de la Nouvelle-Zélande auprès de l'Organisation des Nations Unies

La Nouvelle-Zélande tient à remercier l'Estonie d'avoir saisi le Conseil de l'importante question qu'est celle du maintien de la paix et de la sécurité internationales dans le cyberespace.

Les cybermenaces sont pour tous les États Membres un problème pressant et omniprésent. Elles portent lourdement atteinte à la prospérité et la sécurité de la Nouvelle-Zélande ainsi qu'à la paix et à la sécurité internationales.

Nous devons agir collectivement pour construire un environnement en ligne stable et sûr dans lequel chacune et chacun pourra tirer parti de la connectivité numérique, facteur crucial de développement économique, social et culturel.

Nous apprécions la possibilité qui nous est donnée de donner notre avis sur les efforts internationaux visant à maintenir la paix et la sécurité dans le cyberespace. À cet égard, nous rappelons l'importance critique que revêt le cadre convenu relatif au comportement responsable des États en ligne :

- Nous devons honorer les obligations que nous fait le droit international, dont nous reconnaissons tous qu'elles s'appliquent en ligne aussi bien qu'hors ligne ;
- Nous devons appliquer les normes de comportement responsable des États dans le cyberespace, que nous avons adoptées par la résolution 70/237 de l'Assemblée générale ;
- Nous devons faire en sorte que les mesures de confiance soient largement adoptées et utilisées ;
- Nous devons intensifier nos efforts de renforcement des capacités, de façon à être tous cyberrésilients.

Le cadre nous offre tout ce dont nous avons besoin pour encourager les comportements responsables en ligne, mais son efficacité sera fonction de sa mise en œuvre effective. Nous devons continuer de l'appliquer en pratique, de manière sérieuse et concrète. La Nouvelle-Zélande s'engage à continuer de collaborer à cet égard avec tous les autres États Membres.

Droit international

La Nouvelle-Zélande est un petit État et à ce titre, une partisane fervente du système international fondé sur des règles. C'est particulièrement vrai en ce qui concerne les menaces transfrontières. Notre isolement géographique ne nous met pas à l'abri des cybermenaces.

La Nouvelle-Zélande s'est donnée pour priorité de veiller à ce que le système des Nations Unies soit le héraut d'un environnement en ligne ouvert, sûr, stable, accessible et pacifique et qu'il encourage les États à se comporter de manière responsable dans le cyberespace.

Du point de vue du maintien de la paix et de la stabilité, il est crucial de parvenir à un consensus sur la manière exacte dont le droit international s'applique en ligne. Nous convenons tous que le droit international s'applique aussi bien en ligne que hors ligne. Le droit international applicable recouvre notamment la Charte des Nations Unies, le droit de la responsabilité des États, le droit international humanitaire et le droit international humanitaire.

Nous concédons que des divergences subsistent encore à cet égard. La Nouvelle-Zélande a publié en décembre 2020 une déclaration dans laquelle elle communiquait sa position sur la question de savoir *comment* le droit international s'appliquait en ligne. Nous engageons les autres États Membres à faire part de leurs vues, afin que nous puissions parvenir à une interprétation commune de ces questions et la cerner de manière plus fine.

Normes de comportement responsable des États

La Nouvelle-Zélande est déterminée à prévenir, à détecter, à décourager et à réprimer les cyberactivités malveillantes et à faire respecter les normes de comportement responsable des États telles qu'approuvées dans le rapport de 2021 du Groupe de travail à composition non limitée. Ces normes auxquelles nous avons tous souscrit sont un élément central de la stabilité et de la sécurité du cyberespace. Nous devons continuer à rendre des comptes et à en demander – dans le respect des engagements que nous avons pris.

Nous devons notamment promouvoir la coopération entre les États, protéger les infrastructures critiques, préserver les chaînes d'approvisionnement mondiales, fournir une assistance en cas de besoin, respecter les droits humains et la confidentialité et prévenir l'utilisation malveillante des technologies numériques sur les territoires nationaux.

Nous n'oublions pas combien la pandémie de maladie à coronavirus (COVID-19) a montré qu'il importait d'assurer la sûreté et la sécurité du cyberespace. Partout dans le monde, des activités malveillantes conduites en ligne par des États comme par des acteurs non étatiques ont été signalées. Ces activités ont ciblé notamment des infrastructures de santé critiques, des fonctionnaires engagés dans la lutte contre la pandémie ainsi que des membres du public. Ces faits sont inacceptables et montrent que les menaces cybernétiques mettent des vies en danger. La Nouvelle-Zélande, aux côtés de plusieurs autres États, a publiquement condamné les cyberactivités malveillantes qui ont compromis la riposte à la pandémie.

Mesures de confiance

Nous restons attachés à trouver des solutions constructives, pratiques et concrètes propres à améliorer la cybersécurité sur les plans international et régional. Les mesures de confiance sont à cet égard un outil précieux et nous accueillons avec satisfaction les initiatives pratiques qui favorisent la compréhension mutuelle, la transparence, la prévisibilité et la stabilité dans le cyberespace.

La Nouvelle-Zélande estime que le Forum régional de l'Association des nations de l'Asie du Sud-Est (ASEAN) est une instance clé du dialogue relatif à la cybersécurité régionale. Nous apprécions l'esprit de coopération qui règne entre les membres du forum et attendons avec intérêt de poursuivre notre action avec tous les États Membres dans les années à venir. La Nouvelle-Zélande se réjouit que les enseignements tirés de l'expérience puissent être mis en commun à l'échelle infrarégionale et interrégionale dans l'objectif de renforcer la transparence, la compréhension et la confiance entre partenaires régionaux dans le cyberespace.

Renforcement des capacités

La Nouvelle-Zélande veut contribuer à faire en sorte que tous les États puissent limiter les risques associés au développement de la connectivité, sans rien perdre de ses avantages. Il s'agira notamment de faire comprendre plus largement et plus finement le cadre relatif au comportement responsable des États dans le cyberespace et d'en favoriser la bonne application.

Afin d'atteindre ces objectifs, il faudra veiller à ce que tous les États disposent des outils et des capacités dont ils ont besoin pour participer véritablement aux discussions en cours et aux débats thématiques et pour prendre, aux niveaux national et régional, des initiatives qui serviront la stabilité internationale.

La Nouvelle-Zélande reste déterminée à développer les capacités régionales de cybersécurité, en s'attachant en particulier à collaborer avec ses voisins du Pacifique et de l'Asie du Sud-Est. Nous continuons à exécuter des projets dans le cadre du Programme d'appui en matière de cybersécurité dans le Pacifique, doté de 10 millions de dollars néo-zélandais, et de soutenir le Centre d'excellence pour la cybersécurité, fruit du partenariat entre Singapour et l'ASEAN.

Conclusion

Beaucoup reste encore à faire mais nous ne partons pas de zéro. Nous saluons de nouveau les résultats auxquels ont abouti les travaux du Groupe d'experts gouvernementaux, récemment créé, et du Groupe de travail à composition non limitée. Ces instances et les rapports qu'elles produisent constituent déjà d'importants progrès, qui sont complémentaires et se renforcent mutuellement. Nous devons poursuivre sur cette voie, forts du consensus auquel nous sommes parvenus et des autres accords de consensus adoptés par l'Assemblée générale.

Dans ces discussions, il importe d'entendre des points de vue divers, y compris ceux des petits États et des acteurs non gouvernementaux. Nous nous réjouissons que la question de la cybersécurité suscite largement l'intérêt parmi les États Membres – après tout, la paix et la sécurité dans le cyberespace sont l'affaire de tous. Il est encourageant de voir un si grand nombre d'États s'employer en toute sincérité à régler les problèmes qui se présentent à nous et la Nouvelle-Zélande se tient prête à travailler avec tous en vue de relever le défi.

Annexe XLVIII

Déclaration du Représentant permanent du Pakistan auprès de l'Organisation des Nations Unies

Je tiens à exprimer ma profonde gratitude et à adresser mes remerciements sincères à la Mission permanente de la République d'Estonie, pour avoir convoqué ce débat important et opportun du Conseil de sécurité sur le thème du maintien de la paix et de la sécurité internationale dans le cyberespace.

Les technologies de l'informatique et des communications (TIC) sont porteuses d'un immense potentiel et leur utilité pour la communauté internationale ne fait que croître. Cependant, leur utilisation suscite des questions complexes et fait peser de sérieux risques sur la paix et la sécurité internationales.

L'utilisation des cybertechnologies dans une intention hostile approche rapidement le stade où elle pourrait provoquer une rupture de la paix ou menacer la paix et la sécurité internationales.

L'utilisation abusive et non réglementée des TIC pourrait être lourde de conséquences pour la paix et la sécurité internationale en cas de cyberattaque lancée contre une infrastructure vitale. Certains exemples récents, quoiqu'encore non pleinement avérés, sont parlants.

Il convient de s'attaquer d'urgence à la question de plus en plus pressante de la cybersécurité dans le cadre des efforts plus larges que mènent les Nations Unies en vue de prévenir les conflits.

À cet égard, l'adoption d'un rapport de consensus par le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale en mars de cette année a constitué une avancée historique à l'appui des efforts mondiaux qui sont déployés dans l'optique de créer un environnement numérique sûr, sécurisé, stable et pacifique.

Par l'adoption de ce rapport, la communauté internationale a également réaffirmé sa capacité à se rassembler pour faire face à de grands problèmes mondiaux, dans les circonstances les plus difficiles, telles que la pandémie qui s'est abattue sur nous.

Tout en étant conscients que ce rapport n'a pas apaisé les inquiétudes de tous les États Membres, nous estimons qu'il importe de consolider les progrès faits jusqu'ici, de ne pas se relâcher et de poursuivre ce processus dynamique et transparent.

Le Pakistan a participé de façon positive et constructive aux travaux du Groupe de travail à composition non limitée et se félicite de la mise en place du nouveau Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), créé en application de la résolution 75/240 de l'Assemblée générale.

Ce nouveau Groupe de travail fournit des occasions précieuses de faire des progrès concrets, sur la base des recommandations antérieures, vers le renforcement des règles de comportement responsable dans le cyberespace et la mise en place d'une véritable coopération internationale propre à circonscrire la menace que les utilisations malveillantes des TIC font peser sur la sécurité internationale.

Le Groupe d'expert gouvernementaux, dans son rapport de 2015, et le Groupe de travail à composition non limitée, dans son récent rapport, sont convenus d'un ensemble de conclusions marquantes qui ont contribué à faire émerger, parmi les États Membres, un consensus large autour de l'idée que le droit international, en particulier

la Charte des Nations Unies, était applicable et essentiel au maintien de la paix et de la stabilité de l'environnement numérique.

La Charte des Nations Unies défend sans ambiguïté et de manière catégorique les principes de la souveraineté des États, de leur intégrité territoriale et de la non-ingérence dans les affaires intérieures d'autres États. Ces principes doivent nous guider dans les méandres complexes de la cybergouvernance.

Parallèlement, il convient d'examiner soigneusement à quel point, dans quelle mesure et comment le droit international s'applique au cyberespace et la manière dont il doit être interprété en ce qui concerne le comportement des États et leur utilisation des technologies numériques.

Il ne suffit pas d'affirmer que le droit international existant s'applique au cyberespace pour régler les questions juridiques multidimensionnelles que suscitent ces technologies. Il convient d'adapter le droit au cyberespace en tenant compte de ses caractéristiques spécifiques.

Le Pakistan est conscient qu'il importe d'élaborer un instrument juridique international contraignant adapté aux spécificités des TIC afin de créer un cadre réglementaire qui introduira de la stabilité dans le cyberespace et en assurera la sécurité. Ce cadre juridique doit tenir compte des préoccupations et des intérêts de tous les États, être basé sur le consensus et être développé dans le cadre de l'Organisation des Nations Unies avec la participation active et égale de tous les États.

Les normes volontaires et non contraignantes relatives à l'utilisation responsable des TIC par les États peuvent contribuer à minimiser les risques qui pèsent sur la paix et la sécurité internationales. Cependant, compte tenu des menaces sans précédent qui planent sur l'environnement numérique et des progrès rapides de la technologie, il convient de redoubler d'efforts au niveau international pour établir des règles contraignantes qui contribueront à maintenir la paix et la stabilité et à promouvoir un environnement informatique ouvert, sûr, stable, accessible et pacifique.

Nous devons veiller à ce que le cyberspace ne soit pas exploité pour perpétuer les campagnes de désinformation orchestrées par des États, les incitations à la violence, les discours de haine et les autres formes d'intolérance, notamment l'islamophobie.

L'Organisation des Nations Unies a un rôle central à jouer pour ce qui est de favoriser le dialogue entre les États et la coopération internationale, dans l'optique de faire émerger une vision commune des principaux aspects des questions liées au cyberespace, notamment en ce qui concerne l'application du droit international et des normes, règles et principes de comportement responsable des États, le renforcement de la confiance et la promotion de mesures de transparence, l'appui au renforcement des capacités et la diffusion des meilleures pratiques.

Pour le Pakistan, qui compte plus de 200 millions d'habitants et dont le paysage informatique florissant se caractérise par un nombre croissant d'utilisateurs du numérique, il est extrêmement important d'exploiter les TIC au service du développement socioéconomique, d'une gouvernance plus efficace et plus efficiente et du bon fonctionnement des services publics.

Le Pakistan est déterminé à promouvoir la coopération internationale dans le domaine de l'informatique et de la cybersécurité en tant qu'instrument de réduction de la fracture numérique. Tous les pays sont parties prenantes à part entière de l'élaboration de règles régissant l'économie numérique et la sécurité du cyberespace et des TIC.

Annexe XLIX

Déclaration de la Mission permanente du Pérou auprès de l'Organisation des Nations Unies

[Original : espagnol]

Le Pérou salue l'initiative prise par la présidence estonienne d'avoir convoqué le débat public de haut niveau que nous tenons aujourd'hui au Conseil de sécurité sur un sujet dont l'importance est primordiale et va croissant pour le maintien de la paix et de la sécurité internationales. Nous remercions les intervenants de leurs exposés.

Nous sommes conscients qu'il est utile d'examiner l'utilisation des technologies de l'information et des communications (TIC), de leur évolution rapide et des avantages dont elles sont porteuses dans le contexte de la sécurité internationale. La crise sanitaire causée par la pandémie de maladie à coronavirus (COVID-19) a clairement montré que nous sommes dépendants de ces technologies, qu'il faut d'urgence réduire la fracture numérique et qu'il importe de protéger les infrastructures critiques.

Nous n'ignorons pas les périls que recèle l'utilisation abusive des TIC et qui ajoutent aux risques de conflit dans le cyberespace. L'utilisation malveillante de ces technologies par des groupes terroristes, des organisations criminels, des groupes armés et d'autres agents fait peser de lourdes menaces systémiques sur la paix et la sécurité internationales.

Sachant que ces menaces ne sont pas liées aux technologies en elles-mêmes, mais à la manière dont elles sont utilisées, il nous faut mieux comprendre comment en faire bon usage et comment éviter que l'on s'en serve délibérément à des fins malveillantes, et promouvoir ainsi un cyberespace ouvert, libre, stable et sûr.

C'est dans cet esprit que nous réaffirmons la primauté de la Charte des Nations Unies, fondement solide de l'action en matière de sécurité, et soutenons l'application du droit international et du droit international humanitaire dans le cyberespace. Nous jugeons également qu'il est essentiel de construire en la matière un cadre international fondé sur des obligations juridiquement contraignantes.

Nous apprécions les efforts que fait l'Organisation et les progrès notables qu'elle a faits dans l'élaboration d'éléments visant à promouvoir l'application du droit international, le respect des normes et un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale. Nous nous félicitons ainsi des rapports adoptés par le Groupe de travail à composition non limitée et le Groupe d'experts gouvernementaux et nous espérons qu'en faisant converger les travaux de ces deux instances, nous parviendrons à un discours et à une ligne de conduite uniques et cohérents en matière de cybersécurité.

Nous sommes d'avis qu'au-delà des seuls efforts internationaux, les mesures régionales et nationales, en particulier relatives à la promotion de mesures de confiance, au développement des capacités, à l'échange d'informations et à la mise en commun des meilleures pratiques revêtent une importance fondamentale pour ce qui est de garantir la sécurité dans le cyberespace. Pour les pays comme le nôtre qui accusent des retards technologiques, il est primordial de faire émerger concrètement des interprétations communes et des accords, afin d'éviter que le cyberespace devienne un théâtre de conflit faute que la communauté internationale se soit donné les moyens de se prémunir des risques liés aux TIC.

Compte tenu de la nature interconnectée et de la complexité du cyberespace, du rythme constant de l'innovation dans le domaine des TIC et l'intégration croissante des technologies émergentes, nous sommes partisans de mobiliser le secteur privé, en

particulier l'industrie informatique, la société civile et les milieux universitaires afin de mieux relever les défis qui se présentent à nous. Nous sommes convaincus que leurs contributions continueront d'enrichir les discussions multilatérales sur la question.

En conclusion, nous soulignons qu'il est nécessaire que la communauté internationale dans son ensemble agisse de manière coordonnée et adopte de nouvelles mesures propres à lui faire mieux appréhender les menaces existantes et les modalités de coopération qui permettraient de s'en prémunir. Dans cette entreprise, l'action du Conseil de sécurité, moteur de la prévention des conflits et de l'instauration de la paix et de la sécurité, sera déterminante pour ce qui est de garantir le caractère ouvert, pacifique, sûr et bénéfique d'un cyberespace qui favorise le développement durable et le bien-être des populations.

Annexe L

Déclaration de la Mission permanente de la Pologne auprès de l'Organisation des Nations Unies

Ce tout premier débat public du Conseil de sécurité sur la cybersécurité marque un tournant dans la manière dont nous appréhendons les problèmes qui pèsent sur la paix et la sécurité internationales.

Nous remercions la présidence estonienne et la félicitons de nous avoir donné l'occasion de tenir ce débat très opportun sur les questions de cybersécurité.

En 2019, alors qu'elle siégeait au Conseil, la Pologne avait attiré l'attention des membres de ce dernier sur le problème que constituaient les atteintes à la sécurité informatique au Moyen-Orient.

Il est temps à présent d'appeler l'attention de la communauté internationale tout entière sur la hausse constante des activités malveillantes dans le cyberespace. Depuis 20 ans, en parallèle du développement inouï des technologies numériques, les cyberattaques et les atteintes à la sécurité informatique ne cessent de se multiplier partout dans le monde. Il ne se passe pas un jour sans que la Pologne soit visée.

La nature des faits varie, bien entendu. Certains sont d'origine purement criminelle, d'autres sont motivés par l'appât du gain et d'autres encore, de plus en plus fréquent, relèvent d'une visée politique. On trouve pourtant à ces activités un dénominateur commun : elles sont toutes illégales. Les cyberactivités malveillantes ne peuvent en aucun cas être justifiées ni excusées.

Comme vous l'avez dit très justement dans votre note de cadrage, Madame la Présidente, « Le droit international existant, notamment la Charte [des Nations Unies], fournit aux États des orientations suffisantes pour mener leurs activités [en ligne] ». C'est à la communauté internationale que revient la haute mission d'élaborer collectivement un cadre acceptable régissant la conduite d'activités dans le cyberespace.

La Pologne soutient fermement les travaux accomplis par le Groupe d'experts gouvernementaux et a participé activement à ceux du Groupe de travail à composition non limitée qui a réaffirmé, dans son rapport, que le droit international s'appliquait dans le cyberespace. Nous espérons que la deuxième session du Groupe de travail à composition non limitée contribuera à mieux faire comprendre combien il importe que le cyberespace soit utilisé à des fins pacifiques. Nous attachons également une grande importance aux travaux du Comité spécial de la Troisième Commission de l'Assemblée générale.

Il ne suffit pas de partager la même évaluation de la situation ; il importe bien davantage encore de mener une action commune et bien ordonnée. La Pologne est donc favorable à ce que de multiples parties prenantes participent au débat international sur la cybersécurité, notamment les organisations non gouvernementales, le secteur privé et le milieu universitaire.

La Pologne est également convaincue que cette tâche importante doit être exécutée au niveau infrarégional. En mobilisant les organisations régionales, les États et les représentants de la société civile, il est possible de créer des instruments utiles au renforcement des capacités ainsi que des mesures de confiance.

Afin de dynamiser les efforts faits aux niveaux mondial et régional, il nous faut mettre en commun nos ressources et nos moyens diplomatiques. C'est dans cet esprit que nous soutenons fermement et prônons la création d'un programme d'action, qui

nous paraît le meilleur format de coopération internationale en matière d'activités menées dans le cyberespace.

Nous espérons qu'à la suite du présent débat, la question de la cybersécurité prendra la place qui lui revient et que le Conseil en sera saisi à titre permanent. Le coût politique et économique des activités malveillantes dans le cyberespace est trop élevé pour que cet organe essentiel des Nations Unies n'en fasse pas cas.

Soyez assurés que la Pologne fera tout ce qui est en son pouvoir pour contribuer à tous les processus mondiaux et régionaux, dans l'optique de renforcer l'ordre dans le cyberespace, dans le respect du droit international et des normes convenues en commun.

Annexe LI

Déclaration de la Mission permanente du Qatar auprès de l'Organisation des Nations Unies

[Original : arabe]

Permettez-moi tout d'abord de remercier la Haute-Représentante pour les affaires de désarmement, M^me^ Nakamitsu, de son exposé. C'est notamment grâce aux travaux du Bureau des affaires de désarmement que la cybersécurité prend la place qui lui revient dans le programme de désarmement des Nations Unies.

Nous voyons chaque jour notre monde se transformer à mesure que le cyberespace devient un outil incontournable. Il n'en reste pas moins que les technologies numérique et la connectivité mondiale facilitent aussi l'utilisation abusive du cyberespace. C'est là d'autant plus inquiétant que les infrastructures et services publics vitaux dépendent du numérique. L'utilisation abusive du cyberespace et des technologies de l'informatique et des communications (TIC) par des acteurs gouvernementaux et non gouvernementaux menace la sécurité nationale et nuit à la paix et à la sécurité régionales et internationales ainsi qu'aux relations internationales. De plus, des groupes terroristes exploitent des technologies numériques émergentes pour mieux se livrer à leurs activités criminelles.

Il est évident qu'aucun pays n'est à l'abri de l'utilisation abusive du cyberespace. Il faut donc agir collectivement pour régler ce problème mondial. Fort heureusement, le cyberespace lui-même pourrait être un excellent moyen de coordonner cette action. Comme nous l'avons vu au cours de l'année écoulée, les plateformes numériques sont indispensables à la continuité des travaux des organismes des Nations Unies et d'autres forums de coopération internationale.

Nous devons évaluer les menaces potentielles et l'incidence que pourraient avoir les agissements de pirates informatiques et l'utilisation abusive du cyberespace sur la paix et la sécurité. Face à ces menaces, il nous faut agir ensemble pour renforcer les conditions de sécurité aux niveaux régional et international et promouvoir l'utilisation pacifique du cyberespace et les outils numériques de pointe connexes.

À cet égard, il convient de se pencher avec attention sur la question de l'application du droit international à l'utilisation des TIC par les États et d'engager ces derniers à adopter un comportement responsable dans l'environnement électronique, dans le contexte de la sécurité internationale.

Il faudra, ce faisant, maintenir la libre circulation de l'information et veiller au respect des droits humains et des libertés fondamentales, dans un environnement numérique ouvert, sûr et accessible à toutes et tous.

Les stratégies nationales qui s'ajoutent aux cadres internationaux ont toute leur importance, en ce qu'elles permettent de guider et de coordonner l'action des différentes parties prenantes parmi lesquelles le secteur privé, acteur incontournable des technologies numériques.

La sécurité de l'information et la protection des infrastructures d'information font partie des priorités du Qatar, qui prend des mesures globales et développe ses moyens en matière en s'attachant à promouvoir la coopération internationale et le renforcement des capacités.

La sécurité de l'information et la sécurité informatique sont des questions dont l'Organisation est saisie depuis plusieurs années, mais il lui faut agir pour ne pas se laisser dépasser par l'évolution rapide du monde numérique. Nous nous félicitons donc de l'attention accordée à ce sujet par le Secrétaire général, qui a fait de la

promotion d'un environnement numérique pacifique l'une de ses priorités. Nous nous réjouissons également de voir que le Groupe d'experts gouvernementaux a une nouvelle fois su parvenir à un consensus. Nous attendons avec intérêt la prochaine session du Groupe de travail à composition non limitée, dans la perspective de contribuer à élargir encore le consensus international.

En conclusion, je tiens à dire une nouvelle fois que le Qatar continuera de s'efforcer, à tous les niveaux, à contribuer à l'action menée à l'échelle mondiale en vue de promouvoir la paix, la sécurité et la stabilité dans le cyberespace.

Annexe LII

Déclaration du Représentant permanent de la République de Corée auprès de l'Organisation des Nations Unies, M. Cho Hyun

Je tiens d'abord à vous remercier d'avoir convoqué le débat public opportun que nous tenons aujourd'hui sur le thème du maintien de la paix et de la sécurité internationale dans le cyberespace. Je remercie également la Haute-Représentante pour les affaires de désarmement, M^me^ Nakamitsu, de son exposé approfondi.

En une vingtaine d'années, l'humanité a été le témoin de progrès techniques d'une ampleur inégalée dans le domaine du numérique. Le concept de cyberespace, qui il fut un temps n'existait que dans les livres de science-fiction, est désormais pour nous une réalité du quotidien et nos environnements numérique et physique se fondent en un écosystème unique. Ces progrès ont apporté des avantages économiques et sociaux sans précédents mais nous sommes aussi devenus plus vulnérables face aux cyberactivités malveillantes. Au cours de l'année écoulée, au beau milieu de la pandémie, notre exposition aux cybermenaces a été d'autant plus grande que nous étions plus nombreux en ligne. Qui plus est, la multiplication des cyberattaques contre des infrastructures critiques, notamment des infrastructures et des installations médicales du monde entier, est un sujet de préoccupation croissante.

Dans ce contexte, je voudrais insister sur les quatre points suivants qui revêtent une importance particulière pour ma délégation.

Premièrement, la République de Corée soutient l'action centrale que mène l'Organisation dans les discussions en cours sur les moyens de régler les problèmes qui se présentent et de favoriser le comportement responsable des États dans le cyberespace. À cet égard, ma délégation se félicite de l'adoption du rapport de consensus 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 a présenté cette année, et du quatrième rapport de consensus du Groupe d'experts gouvernementaux, adopté le mois dernier. Ces résultats témoignent des progrès accomplis dans la construction et l'évolution du cadre relatif à l'utilisation responsable des technologies de l'informatique et des communications (TIC) par les États et les processus dont ils sont le fruits ont permis à la communauté internationale dans son ensemble de mieux appréhender les enjeux de ce domaine critique.

Comme tous les États Membres l'ont admis par consensus dans le précédent rapport du Groupe de travail à composition non limitée, le droit international s'applique à l'utilisation des TIC par les États, qui devraient se conformer au cadre relatif au comportement responsable des États lorsqu'ils utilisent ces technologies, comme le Groupe d'experts gouvernementaux l'a souligné dans ses rapports. La primauté du droit international et l'ordre fondé sur les règles doivent prévaloir dans le cyberespace comme dans le monde physique ; c'est une question de paix et de sécurité.

Deuxièmement, ma délégation apprécie grandement le récent rapport de consensus du Groupe d'experts gouvernementaux, qui a permis de cerner mieux encore les normes de comportement responsable des États, les mesures de confiance, le renforcement des capacités et la manière dont le droit international s'applique à l'utilisation des TIC par les États. Dans son rapport, le Groupe d'experts a réaffirmé l'applicabilité du droit international, notamment de la Charte des Nations Unies, et notamment celle du droit international humanitaire dans les situations de conflit armé. La République de Corée est également une tenante convaincue de la recommandation formulée par le Groupe d'experts gouvernementaux selon laquelle les États parties à

tout différend international, y compris en lien avec l'utilisation du numérique, doivent en rechercher la solution, avant tout, par des moyens pacifiques tels que décrits à l'Article 33 de la Charte.

Ma délégation se réjouit en particulier de voir que la norme selon laquelle les États ne devraient pas sciemment permettre que leur territoire soit utilisé pour commettre des faits internationalement illicites au moyen des technologies numériques ait été étoffée dans le rapport. Selon ce principe de « diligence raisonnable », pris en compte dans le rapport de 2015 du Groupe d'experts gouvernementaux sur la suggestion de la République de Corée, chaque État doit prendre des mesures adaptées et raisonnables en réaction à tout fait internationalement illicite dont il aurait connaissance ou qui lui serait notifié.

Troisièmement, nous devons en faire davantage pour renforcer la confiance et parvenir à une vision commune. En tant qu'État membre responsable et nation chef de file du secteur du numérique et des technologies, la République de Corée participe activement aux divers forums régionaux et multilatéraux et contribue à leurs travaux. La semaine dernière encore, le 22 juin, en coopération étroite avec l'Organisation pour la sécurité et la coopération en Europe, elle a organisé avec succès la troisième Conférence interrégionale sur la cybersécurité et la sécurité informatique, consacrée à l'examen des tendances en matière de cybersécurité et visant à promouvoir la coopération entre organisations régionales en la matière. Elle a également organisé la 19e Conférence ONU-République de Corée sur les questions de désarmement et de non-prolifération, centrée sur le développement et les incidences des technologies émergentes en 2020, et assurera la coprésidence de la réunion intersession du Forum régional de l'Association des nations de l'Asie du Sud-Est sur la sécurité informatique pour la période 2021-2023. De plus, en novembre de cette année, la République de Corée lancera un forum international destiné à dynamiser les discussions sur les moyens de lutter contre les menaces émergentes telles que les cyberattaques et l'utilisation malveillante des nouvelles technologies dans le contexte de la paix et de la sécurité internationales. Guidé par les principes d'inclusion, de transparence et d'ouverture, ce forum constituera une plateforme internationale ouverte et accessible à de multiples parties prenantes.

Quatrièmement, nous ne saurions trop insister sur le fait qu'il convient d'adopter une approche multipartite en matière de cybersécurité, compte tenu des multiples domaines et disciplines que recoupe la question du cyberespace et de la sécurité internationale. Les gouvernements restent évidemment au cœur de l'action mais pour que le processus soit efficace, il faudra également mobiliser d'autres acteurs clés, tels que le secteur privé, le milieu universitaire, la société civile et les spécialistes techniques. Nous devons également garder à l'esprit que le dialogue avec d'autres parties prenantes peut grandement faciliter la construction d'une vision commune et l'application du cadre de comportement responsable dans le cyberespace.

En conclusion, je voudrais saisir cette occasion pour réaffirmer l'engagement de la République de Corée à travailler en collaboration avec l'Organisation et tous ses États Membres pour promouvoir un cyberespace ouvert, sûr, stable, accessible et pacifique.

Annexe LIII

Déclaration de la Mission permanente de la Roumanie auprès de l'Organisation des Nations Unies

Nous félicitons l'Estonie d'avoir pris l'initiative d'organiser le tout premier débat public consacré à la cybersécurité et d'avoir saisi formellement le Conseil de cette question précise. Il s'agit là d'un geste opportun, propre à consolider encore l'ordre international fondé sur des règles et notre coopération multilatérale dans un domaine qui revêt la plus haute importance du point de vue du maintien de la paix et de la sécurité internationales.

Le débat que nous tenons aujourd'hui témoigne des progrès remarquables qu'ont fait les États Membres depuis la publication des derniers rapports de consensus du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée en ce qui concerne le renforcement du cadre normatif relatif au comportement responsable des États dans le cyberespace, fondé sur le droit international, les normes établies, les mesures de confiance et le renforcement des capacités.

Face à l'évolution constante des conditions de sécurité sur le plan international, les technologies de l'informatique et des communications (TIC) sont porteuses à la fois d'avantages immenses et des risques les plus aigus et les plus graves. La menace provient aussi bien d'États que d'acteurs non étatiques et pèse sur une série de secteurs clés, tels que l'énergie, le transport, la finance et la santé, qui tous dépendent d'infrastructures physiques et numériques essentielles pour assurer la fourniture de services au niveau national, régional et mondial. Les technologies numériques sont aussi parfois utilisées pour tenter d'affaiblir les institutions démocratiques et de saper la confiance placée par le public dans les principes de la démocratie. Elles peuvent également l'être pour exploiter des vulnérabilités systémiques et servir des objectifs géopolitiques. La pandémie de maladie à coronavirus (COVID-19) est un exemple frais et poignant des effets dévastateurs qu'ont les cyberopérations visant à compromettre ou à altérer les données stratégiques concernant la recherche et la distribution de vaccins.

Dans ces circonstances, on ne saurait donner trop d'importance à la coopération multilatérale entre États responsables, ni au renforcement des partenariats entre les administrations publique, le secteur privé, la société civile et le milieu universitaire. Nous devons œuvrer ensemble pour mettre en commun des données fiables, exactes, à jour et dignes de foi sur les menaces et les moyens d'y riposter de manière crédible, coordonner notre action et renforcer les mécanismes de prévention compétents à l'échelle globale, régionale et nationale. Plus important encore, nous devons nous concentrer sur le renforcement de la résilience de nos sociétés face aux incidences que ces menaces pourraient avoir sur nos infrastructures – aussi bien physiques que numériques et institutionnelles.

Dans ce contexte, il convient de noter que la Roumanie, qui assure actuellement la présidence de la Communauté des démocraties, a fait du lien entre technologie et processus démocratiques une de ses grandes priorités ; en tant que pays hôte du tout nouveau Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, installé à Bucarest, la Roumanie se félicite des projets de partenariats d'investissements en cogestion faisant intervenir les États membres de l'Union européenne et le secteur privé et les soutient activement ; en sa qualité d'hôte du Centre euro-atlantique pour la résilience, récemment créé à son initiative, la Roumanie s'emploiera à générer des idées et des stratégies nouvelles devant permettre aux sociétés de s'adapter aux nouveaux problèmes qui menacent la paix, la sécurité et la stabilité démocratique.

En tant qu'État membre de l'Union européenne, la Roumanie s'attache à promouvoir et à mettre en œuvre les principaux éléments de la nouvelle Stratégie de cybersécurité de l'Union européenne pour la décennie numérique, en particulier la boîte à outils cyberdiplomatique et les moyens de dissuasion et de communication stratégiques qui y sont proposés dans le cadre de la lutte contre les cyberactivités malveillantes. Cette boîte à outils cyberdiplomatique sera un instrument précieux de prévention, de dissuasion et de lutte contre les cyberincidents qui portent atteinte à la sécurité de l'Union et de ses États membres.

La Roumanie envisage la cybersécurité comme une dimension cruciale de la sécurité nationale et s'efforce de concevoir un cadre juridique national adéquat et d'adapter les dispositions existantes afin de faciliter la coopération et l'échange d'informations efficace entre les autorités compétentes et d'honorer ses obligations internationales. Le comportement responsable des États recouvre une série de grandes obligations positives : il s'agit de disposer d'une législation interne, de cyberstratégies et d'institutions modernes et efficaces, de promouvoir la coopération internationale sur les questions de fond et de s'y associer, et, élément crucial, d'agir dans la transparence, d'observer les normes convenues, de défendre les principes démocratiques et de respecter pleinement la dignité humaine.

La Roumanie a fait de la sécurité du cyberespace l'une de ses principales priorités politiques et diplomatiques et cherche à la garantir en favorisant un comportement responsable des États et en consolidant les mécanismes préventifs et normatifs aux niveaux mondial, régional et national. Nous sommes déterminés à promouvoir un cyberespace mondial libre, ouvert, sûr et sécurisé où s'appliquent pleinement les droits humains et les libertés fondamentales et où règne l'état de droit. Nous estimons également qu'il ne peut y avoir d'environnement numérique ouvert, sécurisé, stable, accessible et pacifique sans cadre international fondé sur des règles et basé essentiellement sur le droit international.

La Roumanie a participé activement aux travaux des deux instances des Nations Unies chargées de consolider ce cadre relatif à la cybersécurité (à savoir le Groupe d'experts gouvernementaux et le Groupe de travail à composition non limitée), qui ont réussi à conclure leurs travaux en convenant de recommandations d'importance pour la prévention des conflits dans le cyberespace (concernant notamment la compréhension approfondie de la manière dont le droit international s'applique dans le cyberespace, les normes volontaires non contraignantes de comportement responsable des États et les modalités selon lesquelles le dialogue sur la question pourrait être institutionnalisé).

Pour l'avenir, la Roumanie estime que la création d'un programme d'action pour la promotion d'un comportement responsable des États dans le cyberespace favoriserait l'adoption de mesures pratiques et concrètes de renforcement des capacités et de la confiance et faciliterait l'accès à des sources de financement ouvert, inclusif, transparent et permanent, et aiderait ainsi tous les États Membres à prévenir les conflits, à parvenir à une compréhension commune des menaces et à renforcer leur cyberrésilience.

La Roumanie défendra activement la position qui est la sienne, à savoir que le droit international s'applique au cyberespace, dans le cadre de tous les processus des Nations Unies à venir. Elle est absolument convaincue qu'il n'y a aucune raison de penser que le droit international existant ne pourrait pas correctement régir les relations interétatiques entretenues dans le cyberespace ou par son intermédiaire. Elle estime notamment que le droit international humanitaire s'applique aux cyberopérations menées dans le cadre d'un conflit armé (international ou non international). Dans ces circonstances, les cyberopérations doivent être planifiées et

conduites conformément aux principes régissant la conduite des hostilités, à savoir les principes de distinction, de proportionnalité, de nécessité et de précaution.

Cela étant, l'approfondissement du dialogue et des échanges entre les États peut aider à éclaircir certains aspects précis de la manière dont le droit international s'applique au cyberespace. À cet égard, nous faisons observer que la Roumanie a publié son avis préliminaire sur la question afin de contribuer aux travaux du Groupe d'experts gouvernementaux, en application de la résolution 73/266 de l'Assemblée générale.

Annexe LIV

Déclaration de la Mission permanente du Sénégal auprès de l'Organisation des Nations Unies

[Original : français]

Je voudrais d'abord remercier M^me^ Kaja Kallas, Première Ministre de la République d'Estonie, pour sa présidence de cet important débat public virtuel de haut niveau sur la cybersécurité, un sujet qui prend de plus en plus d'importance dans le système des Nations Unies au regard des menaces sécuritaires grandissantes notées dans le cyberespace.

Je remercie également la Haute-Représentante des Nations Unies pour les affaires de désarmement, M^me^ Izumi Nakamitsu, dont l'intervention a été suivie avec beaucoup d'intérêt par ma délégation.

Le constat est sans appel : la prolifération des activités malveillantes dans le cyberespace constitue une véritable menace pour la paix et la sécurité internationales et interpelle le Conseil de sécurité. Le débat qui nous réunit aujourd'hui traduit une prise en compte de cette menace par le Conseil et reste dans le prolongement des efforts inlassables entrepris depuis plus d'une décennie par l'Assemblée générale en matière de cybersécurité.

Dans cet esprit, les différents processus de réflexion menés dans le cadre des quatre Groupes d'experts gouvernementaux et du Groupe de travail à composition non limitée, respectivement, sur le comportement responsable des États dans le cyberespace et sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, sont salutaires et constituent un signal sans équivoque de la volonté des États de trouver un consensus sur les modalités de régulation du cyberespace.

En reconnaissant l'applicabilité de plusieurs principes et normes du droit international existant et en proclamant la responsabilité des États pour les actes internationalement illicites qu'ils commettraient dans le cyberespace, les conclusions des rapports du Groupe de travail à composition non limitée et du dernier Groupe d'experts gouvernementaux, adoptés, respectivement, en mars et en mai 2021, constituent une contribution supplémentaire à la compréhension de l'exercice du droit international au cyberespace.

En outre, à l'instar de plusieurs pays, le Sénégal estime que les mesures de confiance et de transparence sont indispensables pour promouvoir un comportement responsable des États dans le cyberespace et devraient, à ce titre, être renforcées.

En effet, par des échanges d'informations réguliers sur leurs activités cybernétiques, les États peuvent contribuer à éviter les erreurs de perception et les malentendus, à prévenir et à gérer les crises nées de l'utilisation du cyberespace et, le cas échant, à jeter les bases d'une coopération fructueuse sur le numérique.

Cependant, en raison de l'évolution fulgurante notée dans le secteur et de l'émergence de nouvelles cybermenaces, le Sénégal est d'avis que les règles du droit international positif et les mesures de confiance et de transparence ne suffiraient pas, à elles seules, pour réguler convenablement le cyberespace. Ainsi, elles devraient être complétées par un instrument juridique international contraignant.

Dès lors, une approche générale alliant des mesures de confiance et de transparence volontaristes et une convention internationale contraignante devient pertinente, non seulement pour établir les règles du cyberespace, mais aussi pour prendre en compte les positions et les intérêts de tous les États Membres. C'est vers

cette approche que devront être orientées les réflexions du nouveau Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

Pour sa part, le Gouvernement sénégalais est résolument engagé à contribuer positivement à la réalisation de ce chantier qui demeure une priorité pour lui depuis l'adoption, en novembre 2017, de la Stratégie nationale de cybersécurité 2022. Ce document, dont la vision est d'instaurer « en 2022 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous », comprend une évaluation du contexte stratégique de la cybersécurité au Sénégal prenant en compte les menaces actuelles et futures et définit cinq objectifs stratégiques. Il s'agit du renforcement du cadre juridique et institutionnel de la cybersécurité ; de la protection des infrastructures d'information critiques et des systèmes d'information de l'État ; de la promotion d'une culture de la cybersécurité ; du renforcement des capacités et des connaissances techniques en cybersécurité dans tous les secteurs ; et de la participation aux efforts régionaux et internationaux de cybersécurité.

Conformément à ce dernier objectif, le Sénégal a été le premier pays à être partie à la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (dite Convention de Malabo). Il a aussi adhéré à la Convention sur la cybercriminalité du Conseil de l'Europe, également connue sous le nom de Convention de Budapest, et à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108 du Conseil de l'Europe, STE n° 108) ainsi qu'à son Protocole additionnel sur les autorités de contrôle et les flux transfrontières de données (STE n° 181). En outre, il a adopté la directive de la Communauté économique des États de l'Afrique de l'Ouest sur la lutte contre la cybercriminalité, du 19 août 2011, et endossé l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, du 12 novembre 2018, et l'Appel à l'action de Christchurch contre le terrorisme et l'extrémisme violent en ligne, du 15 mai 2019.

Au plan interne, mon pays s'est doté d'un cadre juridique de régulation de l'utilisation du numérique. Outre la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, on peut citer la loi d'orientation n° 2008-10 du 25 janvier 2008 sur la société de l'information, les lois n° 2008-11 et n° 2008-12 du 25 janvier 2008 sur la cybercriminalité et sur la protection des données à caractère personnel, et la loi n° 2018-28 du 28 novembre 2018 portant code des communications électroniques. Dans le même sillage, le Code de procédure pénale a été révisé pour prendre en compte la procédure en matière d'infractions commises au moyen des TIC.

Parallèlement, l'architecture institutionnelle a été renforcée avec la création du Service technique central des chiffres et de la sécurité des systèmes d'information, de la Division spéciale de lutte contre la cybercriminalité et de la Commission de protection des données personnelles. Cette architecture devrait bientôt s'enrichir de la mise en place d'un comité consultatif national sur la cybersécurité et d'une structure nationale de cybersécurité chargée de conduire la mise en œuvre de la Stratégie nationale de cybersécurité 2022.

En outre, le renforcement des cybercapacités constitue un autre défi à relever, surtout pour les pays en développement. C'est pourquoi, de multiples efforts ont été consentis par le Sénégal en matière de formation sur la sécurité informatique. Ainsi, mon pays compte, à ce jour, plusieurs établissements de formation en la matière, dont les plus illustres sont l'École nationale de cybersécurité à vocation régionale de Dakar, ouverte depuis novembre 2018, et l'Institut professionnel pour la sécurité informatique, créé en octobre 2015.

La cybersécurité ne doit pas freiner l'innovation et les opportunités de développement qu'offrent les nouvelles technologies de l'information et des

communications ou être employée à des fins de restriction du développement desdites technologies.

En tant que moyens de prévention et de lutte contre les utilisations malveillantes du cyberespace, les initiatives de cybersécurité doivent avoir pour but ultime la promotion d'un environnement numérique accessible, sûr, pacifique et prospère, qui ne laisse personne pour compte, conformément à la cible 9.c de l'objectif 9 de l'Agenda 2030.

C'est conscient de cette ambition que le Gouvernement sénégalais a élaboré la Stratégie « Sénégal numérique 2016-2025 », conformément au Plan Sénégal émergent. Ce document, qui incarne l'ambition du Sénégal de maintenir une position de pays leader innovant en Afrique dans le domaine du numérique, est articulé autour du slogan « le numérique pour tous et pour tous les usages en 2025 au Sénégal avec un secteur privé dynamique et innovant dans un écosystème performant ».

Annexe LV

Déclaration du Représentant permanent de Singapour auprès de l'Organisation des Nations Unies, M. Burhan Gafoor

Nous vous remercions d'avoir convoqué cet important débat dans le cadre duquel le Conseil se penchera pour la toute première fois de manière formelle sur la question de la cybersécurité.

Il est grand temps d'aborder ce sujet. La transition numérique s'est accélérée sous l'effet de la pandémie de maladie à coronavirus (COVID-19) et nous a apporté de nouveaux avantages au quotidien, mais nous a aussi exposé à des risques nouveaux. Les cybermenaces et cyberactivités malveillantes se font de plus en plus fréquentes et de plus en plus sophistiquées, et la gravité de leurs conséquences ne fait que croître. On estime que le montant des pertes causées par des cyberactivités malveillantes en 2020 atteint presque les 1 000 milliards de dollars. La multiplication récente de ces agissements nous rappelle avec force que la communauté internationale doit continuer de se prémunir de ces menaces mondiales et transfrontières et être prête à riposter. Je souhaite à cet égard souligner cinq points.

Premièrement, nous devons reconnaître que la question du cyberespace est une question de gestion de l'indivis mondial. En tant que petit État, Singapour a toujours été partisane d'un système multilatéral fondé sur des règles ancrées dans le respect du droit international. Notre approche reste la même en ce qui concerne le cyberespace. Afin que le cyberespace soit sécurisé, sûr, ouvert et interopérable, il nous faut adopter une stratégie mondiale, fondées sur des règles et normes mondiales et sur le respect du droit international. Le défi est de taille, compte tenu de la volatilité et du désordre causés, à l'échelle mondiale, par des tensions géopolitiques croissantes. Mais nous n'avons pas le choix : il nous faut continuer à plaider et à défendre l'applicabilité du droit international et des normes si nous voulons encourager les États à adopter un comportement responsable dans le cyberespace. Nous devons redoubler nos efforts de coopération internationale au service de la cyberrésilience et de la stabilité.

Singapour est attachée au rôle que l'ONU, unique forum universel, inclusif et multilatéral, joue dans l'élaboration de règles applicables au cyberespace. Nous trouvons encourageant de voir que le débat sur la sécurité mûrit à l'Organisation. Depuis la première fois que celle-ci a été saisie de la question de la sécurité des technologies de l'informatique et des communications, en 1998, six Groupes d'experts gouvernementaux se sont penchés sur les risques posés par l'utilisation abusive de ces technologies dans le contexte de la sécurité internationale et sur les moyens de s'en prémunir. Quatre de ces groupes, dont le plus récemment créé, qui vient de conclure ses travaux, ont publié des rapports de consensus.

Les discussions sur la cybersécurité ont été portées à l'attention de tous les États Membres pour la première fois à la soixante-treizième session de l'Assemblée générale, avec la création du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Le succès que constitue l'adoption récente du rapport de consensus du Groupe de travail à composition non limitée est encourageant. Dans ce rapport, qui contribue à forger une compréhension commune de bien des questions, le Groupe de travail recense plusieurs domaines qui doivent être examinés plus avant.

Singapour a participé activement aux travaux des deux Groupes de travail à composition non limitée ainsi qu'à ceux du récent Groupe d'experts gouvernementaux. Elle est honorée d'avoir été choisie pour assurer la présidence du nouveau groupe de travail à composition non limitée sur la sécurité du numérique et

de son utilisation (2021-2025). Dans l'exercice de cette présidence, Singapour restera déterminée à poursuivre les discussions ouvertes, inclusives et transparentes menées à l'Organisation des Nations Unies sur la question de la cybersécurité. Nous espérons que les travaux du nouveau Groupe de travail à composition non limitée contribueront à instaurer un ordre multilatéral fondé sur des règles dans le cyberespace qui apportera à tous les États, petits et grands, la confiance, la prévisibilité et la stabilité qui sont les conditions essentielles du progrès économique, de la création d'emplois et de l'adoption des nouvelles technologies. Nous attendons avec intérêt de travailler en étroite collaboration avec tous les États Membres dans cette entreprise.

Deuxièmement, tous les États sont exposés à des cyberactivités malveillantes qui se font de plus en plus vastes et sophistiquées, mais les petits États, notamment les pays en développement et les pays les moins avancés, sont particulièrement vulnérables. Si nous voulons réellement définir une approche globale en matière de sécurité, nous devons continuer de nous concentrer sur le renforcement des capacités des pays qui en ont besoin. C'est là un domaine dans lequel l'Organisation peut jouer un rôle de coordination. En partenariat avec le Bureau des affaires de désarmement, Singapour a conçu un programme de formation en ligne ouvert à tous les États Membres et visant à mieux faire comprendre les utilisations des technologies de l'informatique et des communications (TIC) et leurs incidences sur la sécurité internationale. Nous sommes résolus à continuer de collaborer avec l'Organisation et à l'aider à proposer d'autres programmes de renforcement des capacités.

Troisièmement, Singapour est convaincue qu'il est possible d'en faire plus pour faire mieux connaître et mieux appliquer les 11 normes volontaires non contraignantes relatives à l'utilisation responsable des TIC par les États. Nous sommes partisans de la mise en commun des meilleures pratiques et des expériences concernant la mise en œuvre de ces normes. Cet exercice permettra de repérer les problèmes auxquels nous devons nous attaquer et les lacunes que de nouvelles normes pourraient devoir combler. Singapour est favorable à l'étoffement des normes existantes. Les activités malveillantes visant des infrastructures d'information critiques transfrontières, telles que le cloud et les systèmes bancaires, peuvent perturber lourdement la fourniture de services essentiels dans plusieurs États, y compris les services liés au commerce international, au transport et aux communications. Les États devraient réfléchir aux moyens d'améliorer la coopération transfrontières, en collaboration avec les propriétaires et les exploitants de ces infrastructures, afin de renforcer les mesures de sécurité qui y sont appliquées.

Cette réflexion m'amène à mon quatrième point, qui concerne le renforcement de la coopération avec les autres parties prenantes et en particulier le secteur privé. Sachant qu'une grande partie des infrastructures d'information critiques relèvent du secteur privé, la communauté internationale doit trouver des moyens de coopérer étroitement avec les intervenants de ce secteur en vue de prévenir et d'atténuer les perturbations liées aux activités malveillantes. Singapour est favorable à l'adoption d'une approche collaborative par laquelle le secteur public et le secteur privé mettraient en commun leurs meilleures pratiques à l'appui d'un cadre de cybersécurité robuste.

Cinquièmement, Singapour est d'avis que les organisations régionales jouent en rôle essentiel en soutenant les discussions lancées à l'Organisation des Nations Unies et en accompagnant la mise en œuvre des règles et normes élaborées sous ses auspices. La cybersécurité était au rang des priorités que Singapour s'était données dans le cadre de sa présidence de l'Association des nations de l'Asie du Sud-Est (ASEAN), en 2018. La même année, l'ASEAN est devenue la première organisation régionale à souscrire en principe aux 11 normes volontaires non contraignantes relatives à l'utilisation responsable des TIC par les États. Elle élabore actuellement

un plan d'action relatif à la mise en œuvre de ces normes. Singapour a soutenu la mise en place de programmes de renforcement des capacités à l'ASEAN comme à l'ONU, comme en témoigne la création, en 2019, du Centre d'excellence ASEAN-Singapour pour la cybersécurité, centre multidisciplinaire de renforcement des capacités dans des domaines tels que les mesures de confiance, la politique, la stratégie, le droit et les questions techniques. Nous attendons avec intérêt de collaborer avec les États Membres en vue de consolider notre action collective de renforcement des capacités informatiques.

Qu'il me soit permis de conclure en disant que c'est sur une infrastructure numérique sûre et sécurisée que doivent reposer nos ambitions concernant l'économie numérique. Il importe plus que jamais que les États Membres s'attaquent ensemble à la question de la cybersécurité, de manière constante, holistique et coordonnée. Singapour se tient prête à collaborer avec tous les États en vue de nouer des partenariats et une coopération au service de l'instauration d'un cyberespace sécurisé, sûr, ouvert et interopérable.

Annexe LVI

Déclaration du Représentant permanent de la Slovaquie auprès de l'Organisation des Nations Unies, M. Michal Mlynár

La Slovaquie souscrit à la déclaration de l'Union européenne. Nous voudrions faire quelques remarques supplémentaires à titre national.

Je tiens à remercier la Présidente d'avoir organisé ce débat pertinent qui nous donne l'occasion de réfléchir aux risques croissants liés aux activités malveillantes dans le cyberespace et à leurs incidences sur la paix et la sécurité internationales, et d'examiner les mesures prises au niveau mondial pour promouvoir la paix et la stabilité dans le cyberespace.

Face à la crise de la COVID-19, il est devenu plus urgent que jamais de renforcer la sécurité et la stabilité du cyberespace. La crise sanitaire a montré que les capacités numériques étaient devenues indispensables à la fourniture de services essentiels et au maintien d'une gouvernance efficace. L'interruption du fonctionnement des infrastructures critiques pourrait avoir de graves conséquences. Les actes de malveillance informatique contre des secteurs et des services vitaux ont des effets déstabilisateurs et pourraient à terme menacer la paix et la sécurité internationales.

Les cybermenaces étant en grande partie de nature transnationale, il est important de maintenir la coopération internationale et le dialogue entre les États, ainsi qu'entre les États et l'ensemble des autres parties prenantes. C'est grâce au partage des responsabilités et aux efforts conjoints des gouvernements, du secteur privé et de la société civile que l'on pourra soutenir efficacement le maintien de la paix et de la sécurité internationales dans le cyberespace et protéger les droits humains.

L'Organisation des Nations Unies joue un rôle important dans la conduite des débats internationaux visant à mieux faire comprendre les problèmes qui se posent dans la sphère cybernétique sous l'angle de la paix et de la sécurité internationales et à favoriser le comportement responsable des États dans le cyberespace.

La Slovaquie est une fervente partisane du multilatéralisme, qui facilite la gestion et le règlement des problèmes actuels et futurs ayant trait au cyberespace. Nous sommes convaincus que la stabilité du cyberespace doit passer par le respect strict du droit international existant, y compris la Charte des Nations Unies dans son intégralité, du droit international humanitaire et du droit international des droits humains. La Slovaquie souscrit pleinement à l'idée que le droit international existant s'applique au comportement des États dans le cyberespace, comme indiqué dans les trois rapports de consensus des Groupe d'experts gouvernementaux approuvés par l'Assemblée générale en 2010, 2013 et 2015. Nous ferons tout notre possible pour mener des discussions transparentes et constructives, et faire en sorte que chacun tire parti de l'expérience, des bonnes pratiques et de l'expertise des autres.

De plus, dans le cadre du Groupe de travail à composition non limitée, la Slovaquie est coauteur du programme d'action visant à favoriser le comportement responsable des États dans le cyberespace. Nous préconisons un dialogue institutionnel inclusif et constructif axé sur les résultats, la régularité et une approche fondée sur le consensus. Nous estimons que le projet de programme d'action constitue précisément l'occasion d'inviter tous les membres de l'Organisation à participer à un tel dialogue.

La Slovaquie considère que les mesures de confiance et de renforcement des capacités en matière informatique sont deux des principaux instruments qui permettront de préserver la stabilité du cyberespace. Les organisations régionales,

telles que l'Organisation pour la sécurité et la coopération en Europe, jouent un rôle très précieux dans la prévention des conflits et le renforcement de la coopération entre les États. La communication et les interactions régulières entre États dans le cyberespace facilitent l'évitement des conflits et l'apaisement des tensions qui pourraient se faire jour. Elles constituent en même temps un cadre de dialogue.

Le droit international est l'une des pierres angulaires de la stabilité et de la prévisibilité des relations entre les États. La Slovaquie se tient résolument aux côtés de ceux qui réaffirment que le droit international existant, en particulier la Charte des Nations Unies dans son intégralité et le droit international humanitaire et le droit des droits de l'homme, s'applique à la conduite des États dans le cyberespace. La Charte définit les règles et principes de droit international qui revêtent une importance particulière pour le maintien de la paix et de la stabilité. Les droits humains valent en ligne aussi bien que hors-ligne, cela ne fait aucun doute, et les États sont tenus de les respecter et de les défendre.

Annexe LVII

Déclaration de la Mission permanente de la Slovénie auprès de l'Organisation des Nations Unies

La Slovénie se félicite de la tenue de ce tout premier débat public thématique du Conseil de sécurité sur la cybersécurité. Il est opportun et utile pour tous les États Membres de se pencher sur la question et le fait d'y consacrer un débat public du Conseil contribue à montrer l'importance qu'elle revêt dans le contexte de la paix et de la sécurité internationales. À cet égard, la Slovénie se félicite des rapports importants adoptés par consensus par le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (Groupe de travail à composition non limitée), qui a été créé récemment, et 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.

Nous nous associons à la déclaration de l'Union européenne et souhaitons faire quelques observations supplémentaires à titre national.

Nous vivons dans un monde interconnecté qui se transforme rapidement. Quand il est global, ouvert, libre, stable et sécurisé, le cyberespace contribue au progrès économique et social. Mais il est aussi le lieu d'actes de malveillance. L'utilisation abusive du cyberespace peut compromettre les secteurs économiques vitaux et aux services essentiels au public, tels que les soins de santé et l'énergie, ainsi que d'autres infrastructures de base. L'utilisation des technologies de l'informatique et des communications (TIC) à des fins malveillantes par des États ou des acteurs non étatiques peut saper la confiance entre les gouvernements et, par ricochet, porter atteinte à la paix et à la sécurité internationales.

La Slovénie croit fermement que si l'on veut atténuer les menaces existantes et émergentes, il faut réglementer le cyberespace dans le plein respect du droit international existant, en particulier de la Charte des Nations Unies dans son intégralité, du droit international humanitaire et des droits humains, et appliquer des normes et règles régissant le comportement responsable des États. Dans cette perspective, notre premier objectif devrait être celui de promouvoir l'application du droit international existant et de concentrer notre action collective sur la mise en œuvre des normes de comportement responsable des États déjà établies, notamment en ce qui concerne la traduction en justice des entités privées opérant depuis une juridiction nationale.

Les normes de comportement responsable des États vont de pair avec les mesures de confiance et de renforcement des capacités. C'est dans ce domaine que nous pouvons vraiment changer la donne. La Slovénie soutient fermement la proposition portée par les 53 États Membres, dont elle-même, consistant à établir un programme d'action visant à favoriser le comportement responsable des États dans le cyberespace, qui fera fond sur les acquis déjà approuvés par l'Assemblée générale. Ce programme d'action sera l'occasion de cultiver des programmes de renforcement des capacités et constituera le mécanisme institutionnel par l'intermédiaire duquel les Nations Unies pourront coopérer et échanger les meilleures pratiques entre elles et coopérer avec d'autres parties prenantes.

De plus, dans le cadre de l'application des normes de comportement responsable des États, la Slovénie continuera à défendre et à soutenir la prise en compte questions de genre, essentielle à la réduction de la « fracture numérique entre les genres » et de promouvoir la participation effective et réelle des femmes aux processus de décision qui intéressent l'utilisation des TIC dans le contexte de la sécurité internationale.

Dans son rôle de présidente du Conseil de l'Union européenne, qu'elle assumera à compter du 1er juillet 2021, la Slovénie renforcera la coopération dans le domaine de la cybersécurité et fera décanter les questions liées au cyberespace intéressant l'Union européenne et la région des Balkans occidentaux. Le rapprochement entre les Balkans occidentaux et le cyberécosystème européen est un aspect important de la mise en place d'un environnement sûr, où règne la confiance, dans lequel on pourra développer le numérique, améliorer la connectivité et élargir l'accès à l'économie et à la société numériques. Il permettra aussi de renforcer la stabilité globale du cyberespace.

Dans cette perspective, la Slovénie prévoit d'organiser le sommet informel Union européenne-Balkans occidentaux au début d'octobre 2021. Elle organisera également une conférence consacrée à la cybersécurité dans les Balkans occidentaux, en coopération avec l'Institut d'études de sécurité de l'Union européenne. De plus, elle contribuera à examiner et à faire progresser la coopération avec les États des Balkans occidentaux en ce qui concerne l'action de prévention et les enquêtes relatives aux atteintes sexuelles et aux actes d'exploitation sexuelles commis contre des enfants.

Quand elle assumera la présidence du Conseil de l'Union européenne, la Slovénie appuiera l'action normative que mène l'Union en vue de renforcer la cyberrésilience et la gestion des crises liées au cyberespace, dans le cadre de l'examen de la Directive sur la sécurité des réseaux et systèmes d'information, dans laquelle sont définies des mesures propres à garantir un niveau de cybersécurité élevé dans tous les États membres, et en s'efforçant de promouvoir activement l'utilisation de la boîte à outils cyberdiplomatique, qui doit contribuer à prévenir les conflits, à atténuer les risques liés à la cybersécurité et à renforcer la stabilité des relations internationales. La Slovénie va s'efforcer d'approfondir la coopération internationale et de réduire les risques de méprise, d'escalade et de conflit.

Pour terminer, je souhaite réaffirmer le rôle central que joue le Conseil de sécurité en soutenant les efforts faits dans le domaine de la cybersécurité, qui sont essentiels au maintien de la paix et de la sécurité internationales. L'organisation même de ce débat public a déjà été une incitation à construire un environnement propre à favoriser la coopération, à renforcer la confiance en matière de technologies numériques et à construire un cyberespace mondial ouvert, libre, stable et sûr.

Annexe LVIII

Déclaration de la Mission permanente de l'Afrique du Sud auprès de l'Organisation des Nations Unies

L'Afrique du Sud a pris note avec intérêt de la convocation de ce débat public dans le cadre duquel le Conseil était appelé, pour la toute première fois, à examiner la question du maintien de la paix et de la sécurité internationales dans le cyberespace comme une question thématique à part entière. Nous remercions également la Haute-Représentante pour les affaires de désarmement, M^me^ Nakamitsu, de son exposé.

Nous avons pris note également des questions directrices qui avaient été communiquées en amont du débat d'aujourd'hui et tâcherons d'y répondre par la présente déclaration.

En premier lieu, l'Afrique du Sud tient à souligner que la question de la paix et de la sécurité dans le cyberespace est omniprésente et complexe et exige l'attention pleine et entière de tous les États Membres de l'Organisation. Nous estimons donc qu'il convient de l'examiner dans le cadre de la Première Commission de l'Assemblée générale, qui a déjà travaillé sur le sujet.

Les États Membres ont participé à ces travaux par l'intermédiaire de plusieurs groupes d'experts gouvernementaux, dont le dernier s'est consacré aux moyens de favoriser le comportement responsable des États dans le cyberspace et a produit un rapport de consensus à la fin mai 2021, sous la direction éclairée de l'Ambassadeur Guilherme de Aguiar Patriota, du Brésil.

De plus, tous les États Membres ont contribué aux travaux du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale de 2019, qui a adopté son rapport de consensus en mars 2021, et à ceux du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), récemment créé et placé sous la direction de l'Ambassadeur et Représentant permanent de la République de Singapour, Burhan Gafoor, qui en assumera la présidence.

Les États Membres de l'Organisation ont donc déjà bien progressé dans l'examen des nouvelles menaces qui pèsent sur la paix et la sécurité internationales dans le cyberespace, des cadres juridiques internationaux qui régissent cette dimension de la paix et de la sécurité, des normes, règles et principes qui guident l'action des États, des mesures de confiance nécessaires, des besoins de renforcement des capacités et des moyens de poursuivre le dialogue dans ce domaine.

Cela étant posé, je souhaite aborder brièvement les quelques points suivants.

L'Afrique du Sud estime que face à la multitude des menaces émergentes, il faut mobiliser toutes les parties prenantes, dont la société civile et le secteur privé. Cela s'impose si nous voulons à la fois comprendre la nature des menaces en question et coopérer à l'échelle de toute la société pour nous prémunir des risques posés par les États et les acteurs non étatiques dans le cyberespace et y opposer une réponse adaptée.

L'Afrique du Sud tient à souligner qu'il faut réduire le fossé numérique et le fossé entre les genres et transformer la fracture numérique, de sorte qu'elle devienne le creuset de possibilités nouvelles qui seront les clefs du renforcement de la résilience et des progrès sur le plan du développement. Cela étant dit, la sophistication croissante des cyberattaques est un sujet d'inquiétude pour les pays en développement tels que le nôtre.

L'Afrique du Sud reste préoccupée par la menace croissante que constituent les cyberattaques contre des infrastructures et infrastructures d'information critiques. Nous estimons qu'il faut répondre à ces menaces en coopérant davantage et créant des mécanismes consacrés aux meilleures pratiques, mais ces efforts doivent être faits à l'appui des priorités nationales et de l'action menée pour identifier et définir lesdites infrastructures. Nous sommes également conscients que les retombées économiques et sociales positives des technologies numériques ne doivent pas être éclipsées par les risques que posent leur utilisation malveillante. Ce ne sont pas ces technologies qui doivent nous inquiéter, mais bien leur utilisation abusive.

Soucieuse de réglementer l'utilisation du cyberespace et de contrer les menaces qui pèsent sur la paix et la sécurité internationales, l'Afrique du Sud soutient l'applicabilité du droit international, en particulier de la Charte des Nations Unies dans son intégralité, dans le cyberespace.

Compte tenu du travail considérable déjà accompli, nous estimons qu'il faut à présent nous concentrer sur la mise en œuvre des normes, règles et principes existants. Il convient de prendre acte d'une vérité fondamentale, que connaissent tous les pays en développement : tous les États ne sont pas exposés au même niveau de risque, puisque tous n'ont pas les mêmes moyens de se prémunir des actes de malveillance dans le cyberespace. Ma délégation souhaite donc souligner qu'il faut que les États et d'autres parties prenantes mettent en place des programmes de renforcement des capacités qui aideront les pays à lutter contre les risques de déstabilisation posés par les acteurs malveillants dans le monde numérique. L'Afrique du Sud estime que le renforcement des capacités est indispensable pour mettre les États sur un pied d'égalité et améliorer ainsi la sécurité de tout le cyberespace, puisqu'il s'agit d'un défi mondial qui exige des solutions mondiales.

Enfin, l'Afrique du Sud reste déterminée à poursuivre la coopération concernant ces questions, en particulier dans le cadre du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, qui commencera ses travaux de fond en décembre. Cette instance constituera une plateforme unique et inclusive de dialogue sur les moyens de lutter contre les menaces nouvelles, complexes et omniprésentes qui pèsent sur la paix et la sécurité internationales dans le cyberespace.

Annexe LIX

Déclaration de la Mission permanente de la Suisse auprès de l'Organisation des Nations Unies

[Original : français]

Je tiens à remercier l'Estonie d'avoir organisé ce débat ouvert, ainsi que la Haute-Représentante pour son intervention. Le cyberespace fait désormais partie intégrante de nos sociétés et crée d'immenses possibilités de développement social et économique. Dans le même temps, les cyberopérations malveillantes présentent un risque d'instabilité et sont devenues une menace pour la paix et la sécurité internationales. Nous sommes préoccupés par le fait que le cyberespace est instrumentalisé pour la projection de puissance et devient de plus en plus fragmenté et déstabilisé.

Un cyberespace ouvert, sûr, stable, accessible et pacifique est bénéfique pour tous. L'Organisation des Nations Unies (ONU) joue un rôle crucial à cet égard. La Suisse se félicite de la récente adoption par consensus des rapports du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée. Ces rapports représentent des étapes essentielles en vue d'un comportement responsable des États dans le cyberespace.

Pour promouvoir la paix et la stabilité dans le cyberespace, j'aimerais souligner quelques points.

Premièrement, le droit international s'applique dans le cyberespace. Son respect est une condition essentielle à la prévention des conflits et au maintien de la paix et de la sécurité internationales. L'obligation de résoudre les différends par des moyens pacifiques s'applique aussi aux activités des États dans le cyberespace. En outre, le droit international humanitaire est applicable lorsqu'un conflit armé, international ou non international, existe de fait. La Suisse se félicite du fait que le dernier rapport du Groupe d'experts gouvernementaux indique cela clairement. Il s'agit d'une étape significative. Le droit international humanitaire et ses principes fondamentaux posent d'importantes limites à l'exécution de cyberopérations dans le contexte de conflits armés.

Deuxièmement, la Suisse s'inquiète de l'impact humanitaire des cyberopérations malveillantes, qui sont à la hausse depuis la pandémie et concernent souvent des infrastructures médicales. La Suisse souligne que celles-ci sont protégées, comme démontré lors du débat ouvert en avril. Les rapports du Groupe d'experts gouvernementaux fournissent un cadre pour protéger les infrastructures critiques contre les activités cyber malveillantes. En outre, les données collectées à des fins humanitaires doivent être protégées. Nous encourageons les États également à respecter les normes facultatives de comportement responsable dans le cyberespace et les orientations supplémentaires du Groupe d'experts pour leur mise en œuvre, pour éviter des dégâts aux infrastructures critiques, mitiger les impacts humanitaires et garantir la protection des civils.

Troisièmement, les mesures de confiance sont importantes pour prévenir un climat de méfiance dans le cyberespace. Au niveau régional, la Suisse s'est engagée à faire progresser le rôle de l'Organisation pour la sécurité et la coopération en Europe pour promouvoir la cyberstabilité. La Suisse élabore, conjointement avec l'Allemagne, une proposition de mise en œuvre d'une mesure de confiance qui prévoit des consultations dans le contexte d'un cyberincident grave. La Suisse s'engage aussi pour la transparence et le renforcement des capacités : notre Centre national pour la cybersécurité fournit un soutien technique aux autres États en cas d'incident et partage des données et informations sur les menaces éventuelles. Le Conseil de

sécurité et les organisations onusiennes devront prendre en compte les initiatives régionales et les mesures de confiance qui se sont avérées utiles pour promouvoir la paix et la stabilité dans le cyberespace.

Finalement, les organisations de la société civile, la communauté académique et technique ainsi que le secteur privé jouent un rôle important dans le soutien à la cyberstabilité internationale, notamment en ce qui concerne le respect des droits de l'homme et des libertés fondamentales en ligne et hors ligne. La Suisse, en tant que membre de la Coalition pour la liberté en ligne s'engage avec plus de 30 gouvernements et un réseau des parties prenantes pour promouvoir la liberté d'expression sur Internet. Nous encourageons le Conseil de sécurité et les États membres à impliquer les différents acteurs dans la mise en œuvre du cadre pour un comportement responsable des États dans le cyberespace.

La coopération multilatérale et l'adhésion au droit international, y compris les droits humains et le droit international humanitaire, sont essentielles pour la paix et la sécurité dans le cyberespace. La Suisse encourage la poursuite des travaux sur ces sujets, y compris au sein du nouveau Groupe de travail à composition non limitée et du futur programme d'action pour la promotion du comportement responsable des États dans le cyberespace. En tant que candidate pour le Conseil de sécurité, la Suisse se réjouit de poursuivre un dialogue multipartite et constructif, sur la base des acquis préexistant.

Annexe LX

Déclaration de la Mission permanente de la Thaïlande auprès de l'Organisation des Nations Unies

La Thaïlande apprécie les efforts que l'Estonie a faits pour organiser ce débat public de haut niveau du Conseil de sécurité sur le maintien de la paix et de la sécurité internationale dans le cyberespace en ce moment tout à fait opportun. Nous saluons également l'esprit d'initiative dont l'Estonie a fait preuve, en étant la première à organiser une réunion formelle du Conseil sur la cybersécurité. Nous espérons que la sécurité du cyberespace et des technologies de l'information et des communications (TIC) et la prévention de leur utilisation malveillante resteront des priorités pour le Conseil et continuons d'inviter tous les membres de l'Organisation à prendre part à ces débats d'importance.

La Thaïlande estime que le cyberespace est un atout pour l'humanité, comme on l'a vu pendant la pandémie, pendant laquelle il a permis aux gens de rester connectés aux services sociaux de base et, plus important encore, de rester en contact les uns avec les autres, et qu'il contribue à la réalisation du Programme de développement durable à l'horizon 2030. Cependant, l'utilisation des TIC à des fins malveillantes par les États et les acteurs non étatiques, y compris des terroristes, par exemple les attaques contre des infrastructures civiles critiques, mettent en péril la paix et la sécurité internationales et compromettent aussi la sécurité de nos populations. Il incombe donc aux États, conformément au droit et aux normes internationales applicables, de s'attaquer à ce sujet.

La Thaïlande est d'avis que l'Organisation peut contribuer fortement à soutenir l'action menée en faveur d'un cyberespace stable et sûr. De fait, la sécurité du cyberespace occupe les États Membres depuis plus de 20 ans. Les progrès les plus évidents tiennent à l'adoption historique, par consensus, du rapport du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (2019-2021) et du rapport 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 (2019-2021).

La Thaïlande se félicite de la création du nouveau Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Nous sommes certains que sous la direction avisée du Représentant permanent de Singapour et Président du Groupe de travail à composition non limitée, Burhan Gafoor, les États mèneront des discussions fécondes, notamment sur les moyens de renforcer la transparence et la confiance et la coopération entre les États et d'étoffer les normes relatives au comportement responsable des États dans le cyberespace.

La Thaïlande espère que les points ci-après pourront être réglés ou éclaircis dans le cadre du nouveau Groupe de travail à composition non limitée : étoffement des normes et recommandations relatives à l'application des normes de comportement responsable des États ; émergence d'une compréhension commune de la manière dont le droit international s'applique dans le cyberespace et repérage d'éventuelles lacunes ; création de mesures de confiance durables et fondées sur la demande et adoption d'un mécanisme de « dialogue institutionnel régulier ».

La Thaïlande prend note également de la contribution positive apportée par d'autres organes gouvernementaux, le secteur privé et les organisations de la société civile et des processus qui ont alimenté l'action collective en faveur d'un cyberespace sûr et sécurisé. Elle est favorable à l'adoption d'une approche multipartite dans le

cadre de cette entreprise, l'objectif étant d'y associer véritablement les parties prenantes et autres partenaires de la société, notamment les femmes et les jeunes.

La Thaïlande soutient donc le renforcement du socle normatif, ce qui passerait par l'amélioration de l'application concrète des normes convenues, la réduction des écarts et des besoins en matière de capacités et le maintien des canaux multilatéraux et bilatéraux dans l'optique de la poursuite du dialogue. Tous les États doivent continuer d'œuvrer ensemble pour préserver la vision partagée d'un cyberespace et d'un environnement numérique ouverts, sûrs, accessibles et pacifiques, pour toutes et tous.

Annexe LXI

Déclaration de la Mission permanente de la Turquie auprès de l'Organisation des Nations Unies

Je tiens à remercier l'Estonie d'avoir organisé ce débat public centré sur un sujet qui revêt une importance critique, tout particulièrement dans le contexte de la pandémie. Je remercie également la Haute-Représentante pour les affaires de désarmement, M^me^ Nakamitsu, de son exposé.

L'utilisation des technologies de l'information et des communications (TIC) façonne l'économie et le développement partout dans le monde. La pandémie a révélé combien nous sommes dépendants des technologies numériques. Il est crucial de veiller à ce que l'accès aux TIC soit libre, ouvert et sûr, cela ne fait aucun doute.

La Turquie s'inquiète de voir croître le nombre de cyberattaques. Les cyberactivités malveillantes ciblant des infrastructures critiques, le terrorisme, l'espionnage numérique, la fraude, les atteintes et les actes d'exploitation sexuelles commis en ligne contre des enfants et l'utilisation abusive de données personnelles, entre autres menaces, compromettent aussi la paix et la sécurité internationales.

Avec les progrès de la technologie, il est devenu plus facile de commettre des cyberattaques, dont les incidences néfastes et le coût pour les victimes se font rapidement plus difficiles à supporter. Les cyberattaques sont aussi de plus en plus ciblées et leur coût annuel augmente de manière exponentielle. Pour se défendre contre ces attaques, il faut être équipé de méthodes et d'outils nouveaux et à jour.

La Turquie se félicite du rapport de consensus adopté par le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et de celui 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, publié plus récemment. Ces rapports sont des ajouts précieux aux travaux menés sur la cybersécurité sous les auspices de l'ONU. Il est également important que les rapports du Groupe de travail à composition non limitée et du Groupe d'experts gouvernementaux soient compatibles et complémentaires, dans la perspective du renforcement de la stabilité, de la résilience et de la coopération internationale dans le cyberespace. Nous espérons voir davantage de cohésion dans cette entreprise à l'avenir.

La Turquie, qui connaît une transformation numérique rapide, s'est attachée à prendre les mesures nécessaires pour améliorer sa cybersécurité. Elle applique actuellement sa Stratégie nationale de cybersécurité et le plan d'action connexe, qui couvrent la période 2020-2023. Les principaux objectifs stratégiques du plan d'action sont la protection des infrastructures critiques et le renforcement de la résilience, le renforcement des capacités, le réseau organique de cybersécurité, la sécurité des technologies de nouvelles générations (par exemple, l'Internet des objets, la 5G, le cloud, etc.), la lutte contre la cybercriminalité, la création et le développement de technologies domestiques et nationales, la prise en compte de la cybersécurité dans les politiques de sécurité nationale et le renforcement de la coopération internationale.

Par ailleurs, l'Équipe turque d'intervention cybernétique d'urgence joue un rôle crucial, en exécutant et en coordonnant les mesures visant à prévenir les cybermenaces.

Ces mesures sont complétées par des programmes de formation et par des exercices de cybersécurité nationaux et internationaux. L'Autorité turque des technologies de l'information et des communications propose de formations publiques en ligne sur la cybersécurité et d'autres domaines connexes. Plus de 5 000

personnes ont ainsi reçu une formation sur la cybersécurité sous ses différents aspects au cours des quatre dernières années.

L'Autorité organise également des activités de sensibilisation, dont la « Journée pour un Internet plus sûr », qui vise à mieux faire connaître les moyens d'utiliser Internet de manière responsable et sûre. De plus, la Turquie agit pour parer l'augmentation des risques liés à la cybersécurité et a pris des mesures, en coopération avec les parties concernées, afin de garantir la continuité des opérations, l'accessibilité du cyberespace et la protection des consommateurs pendant la pandémie.

La Turquie s'est également employée à renforcer le cadre législatif national applicable.

Les cyberrisques ne s'arrêtent pas aux frontières ; il est donc crucial d'approfondir la coopération internationale. Dans cet esprit, la Turquie échange des renseignements sur les cybermenaces et contribue aux politiques et aux stratégies de coopération mises en place par les organisations régionales et internationales, dont l'Organisation pour la sécurité et la coopération en Europe, le G20 et l'OCDE. Elle participe également à des exercices internationaux, notamment ceux qu'organisent l'UIT et l'OTAN.

L'Organisation des Nations Unies est la cheville d'une coopération plus stratégique et plus efficace entre les États en ce qui concerne l'utilisation des TIC. La Turquie soutient que le droit international s'applique dans le cyberespace. Il est grand temps que nous poursuivions les travaux déjà entrepris au sein du système des Nations Unies et trouvions des moyens de faire réellement appliquer les règles, normes, principes et recommandations relatives au comportement responsable des États dans le cyberespace.

À l'avenir, il nous faudra notamment donner la priorité à la construction d'une vision commune de la manière dont le droit international s'applique dans le cyberespace. C'est là une condition essentielle si nous voulons limiter les malentendus et promouvoir le principe de responsabilité dans le cyberespace.

Il faut également établir des voies de communication entre les États Membres en cas d'urgence et les utiliser pour mettre en commun les ressources et les informations. Cela renforcerait considérablement la confiance et accélérerait les efforts de renforcement des capacités.

Il faut de plus examiner et renforcer d'urgence les instruments internationaux existants, afin d'améliorer la coopération dans le domaine des nouvelles technologies telles que le cloud, l'Internet des objets, la 5G et l'intelligence artificielle.

Il pourrait être utile de conduire une étude des approches réglementaires nationales de la sécurité des nouvelles technologies et d'établir des codes de conduite qui encadreraient et éclaireraient les dispositifs nationaux. Il faut en outre faire émerger une vision et des définitions communes des menaces.

En matière de renforcement des capacités, nous estimons que l'ONU et les organisations régionales peuvent promouvoir des programmes d'échange à l'intention des spécialistes de la sécurité et créer des plateformes de formation communes. Il convient d'encourager la conduite d'exercices internationaux afin d'améliorer le niveau de préparation des États face aux problèmes de sécurité informatique et de consolider leurs moyens de riposte.

Le cyberespace ne connaît pas de frontières et la cybersécurité fait intervenir de nombreuses parties prenantes. Aussi les autorités nationales doivent-elles collaborer avec les utilisatrices et les utilisateurs, le secteur privé, les ONG et leurs homologues

internationaux dans le cadre de la lutte contre les cybermenaces. Les fournisseurs, prestataires de services et entreprises de sécurité du monde entier devraient également coopérer plus efficacement avec les gouvernements et les organisations internationales, afin de contribuer à assurer la sécurité du cyberespace à l'échelle mondiale.

La Turquie est déterminée à continuer de coopérer et à poursuivre le dialogue afin de promouvoir la sécurité du cyberespace à l'échelle régionale et mondiale.

Annexe LXII

Déclaration de la Mission permanente de l'Ukraine auprès de l'Organisation des Nations Unies

Nous remercions l'Estonie d'avoir pris l'initiative d'organiser cette importante séance du Conseil de sécurité, ainsi que la Haute-Représentante pour les affaires de désarmement, M^me^ Nakamitsu, de son exposé.

Internet a changé sous l'effet des progrès rapides des technologies de l'information et des communications : plateforme de communication commode, il est aussi véritablement devenu une arme, de plus en plus dangereuse aux mains de hackers, de criminels, de certains acteurs étatiques et de leurs supplétifs.

Malheureusement, et malgré les normes juridiques existantes et les mécanismes internationaux de lutte contre la cybercriminalité établis à l'échelle nationale, régionale et internationale, les avantages du monde numérique moderne n'ont été que trop souvent dévoyés et les cyberattaques de plus en plus fréquemment employées comme une nouvelle méthode de guerre hybride.

Au fil du temps, les cybermenaces en sont venues à menacer la politique internationale. Au cours des dernières années, plusieurs États tombés victimes de cyberattaques en ont payé le prix fort.

Depuis 2014, ces attaques sont l'un des principaux instruments des tentatives externes visant à miner la souveraineté de l'Ukraine. Entre 2014 et 2021, l'Ukraine a fait face à un nombre inouï de cyberopérations visant des éléments vitaux de ses infrastructures critiques. La plupart de ces attaques ont été lancées par des groupes de hackers contrôlés par la Fédération de Russie.

Les cyberopérations visant de grandes infrastructures critiques, les secteurs de l'énergie et des transports et les industries pétrolières et gazières sont un problème majeur et compromettent la paix et la sécurité internationales. Récemment, l'entreprise Colonial Pipeline a fait l'objet d'une cyberattaque qui a gravement touché les équipements informatiques de gestion de son oléoduc et a eu de lourdes répercussions.

Alors que le monde est aux prises avec la pandémie de maladie à coronavirus (COVID-19), on ne voit que trop bien les effets dévastateurs des cyberopérations malveillantes. Certains acteurs étatiques et non étatiques tirent parti de la crise mondiale pour lancer de telles opérations, notamment contre le secteur de la santé. C'est là un sujet d'inquiétude pressant pour la communauté internationale.

Au-delà des seules infrastructures critiques, la politique internationale elle-même est de plus en plus exposée à l'utilisation malveillante de capacités informatiques toujours plus complexes et sophistiquées, comme en témoignent les affaires très médiatisées d'interférence dans des campagnes électorales majeures et les antécédents des candidats faisant intervenir des hackers du Kremlin.

La cyberstabilité est donc devenue un pilier essentiel de la paix et de la sécurité globale et requiert le strict respect du droit international, qui s'applique dans le cyberespace, comme le Groupe de travail à composition non limitée et le Groupe d'experts gouvernementaux l'ont récemment réaffirmé dans leurs rapports, la bonne mise en œuvre des normes, règles et principes de comportement responsable et une coopération internationale renforcée visant à préserver un cyberespace libre, ouvert, stable et sécurisé.

Nous soulignons qu'il faut s'attacher en particulier à établir des points de référence commun dans la lutte contre les cybermenaces, à mutualiser les bonnes

pratiques, à renforcer la confiance dans le domaine de la cybersécurité, à prévenir l'utilisation du cyberespace à des fins politiques, terroristes et militaires, et offrir une assistance technique et financière aux États en vue de leur donner les moyens de résister aux cyberattaques, d'atténuer les risques et d'être plus résilients.

À l'heure actuelle, les cyberopérations visant des infrastructures critiques et des organismes publiques, ainsi que les campagnes de désinformation, parfois constitutives d'incitations au terrorisme, sont souvent utilisées comme des moyens d'interférer dans les affaires internes d'États souverains, dont l'Ukraine.

Il ne fait aucun doute que la Russie utilise les technologies de pointe pour servir ses objectifs politiques et géopolitiques, en soutenant et en alimentant les conflits dans les États voisins et en usant d'une stratégie agressive de cyberguerre.

Nous engageons vivement la communauté internationale à examiner exhaustivement les moyens de faire rendre des comptes à tout État ou tout acteur étatique qui se serait rendu coupable de préparer ou de commettre des actes de malveillance informatique ciblés ou de diffuser de fausses informations à des fins hostiles.

Somme toute, l'action internationale menée dans ce domaine restera vaine sans mécanismes fiables permettant de repérer, de punir et de traduire en justice les personnes et les États qui coordonnent et financent des activités illicites dans le cyberespace mondial.

Annexe LXIII

Déclaration de la Mission permanente des Émirats arabes unis auprès de l'Organisation des Nations Unies

La pandémie de maladie à coronavirus (COVID-19) a montré que le monde dépend des technologies de l'information et des communications, sans lesquelles nous n'aurions pu rester informés et reliés les uns aux autres alors qu'il nous fallait physiquement tenir nos distances.

Au cours des 18 derniers mois, on a vu augmenter le nombre de cyberopérations malveillantes visant des établissements de santé, dont des organismes chargés de faire des recherches et d'élaborer un vaccin contre la COVID-19. Nous vivons dans une région instable et le Moyen-Orient n'est pas à l'abri des risques que constituent ces activités malveillantes ; il est souvent la cible de cyberopérations et d'actes d'espionnage d'ampleur. Ces dernières années, plusieurs problèmes graves ont touché le secteur des télécommunications, le secteur bancaire et le secteur public dans notre région. Les installations pétrolières et gazières ont aussi été prises pour cible et les dégâts causés se sont chiffrés à plusieurs centaines de millions. Susceptibles d'être l'étincelle qui ferait naître un conflit dans un environnement déjà tendu, ces cyberactivités malveillantes contre les infrastructures critiques de la région menacent la paix et la sécurité internationales.

Les Émirats arabes unis sont déterminés à créer les infrastructures et les dispositifs qui leur permettront d'améliorer leurs capacités de cybersécurité, à la fois pour se défendre et pour mieux collaborer avec d'autres et relever les défis qui s'imposent à tous. En novembre 2020, nous avons créé le Conseil de la cybersécurité des Émirats arabes unis, qui va formuler une stratégie nationale de cybersécurité exhaustive et un plan de riposte en cas de cyberattaque. Nous accueillons les principales conférences consacrées à la cybersécurité et à la transformation numérique, dont le GITEX, le GISEC et Cybertech, en vue de renforcer nos capacités nationales, et avons mis en place une plateforme de partenariat public-privé destinée à faciliter la mise en commun des informations. Nous collaborons également avec les États, les organisations internationales et les entités du secteur privé, afin que l'information circule au niveau stratégique et au niveau technique. Les Émirats arabes unis contribuent ainsi aux travaux des organisations régionales, par exemple à la nouvelle plateforme conjointe d'analyse des logiciels malveillants du Conseil de coopération du Golfe, et sont un membre actif de l'équipe d'intervention informatique d'urgence de l'Organisation de la coopération islamique. Ces mesures de coopération, de transparence et de renforcement de la confiance sont l'une des manières dont les Émirats arabes unis contribuent à atténuer les cyberrisques qui pèsent sur la paix et la sécurité internationales.

Les Émirats arabes unis accueillent avec satisfaction les recommandations formulées dans les rapports du Groupe d'experts à composition non limitée et du Groupe d'experts gouvernementaux, dont il ressort clairement qu'il faut soutenir les efforts visant à mieux faire appliquer les normes volontaires de comportement responsable des États dans le cyberespace et parvenir à une compréhension commune de la manière dont le droit international s'applique aux activités menées en ligne. Il convient toutefois d'en faire encore davantage, tant pour encourager les États et les aider à appliquer les recommandations que pour définir de nouvelles orientations, compte tenu de la rapidité avec laquelle l'environnement numérique évolue. Le programme d'action visant à favoriser le comportement responsable des États dans le cyberespace est un plan d'étapes optimal pour les travaux à venir et contribuera à limiter les cyberrisques qui compromettent la paix et la sécurité internationales.

Atténuer ces risques ne sera pas chose facile. Les Émirats arabes unis ont deux recommandations à faire à cet égard.

Premièrement, les États devraient proposer des activités de formation et de renforcement des capacités aux niveaux bilatéral, régional et international, sous la forme de programmes de formation ou d'orientations devant faciliter la mise en œuvre des normes de comportement responsable des États. Ces initiatives peuvent faire office de mesures de confiance, en ce qu'elles limitent la méfiance et les malentendus entre États dans le cyberespace, qui peuvent mettre en péril la paix et la sécurité internationales.

Deuxièmement, les États devraient continuer à communiquer leurs vues et leurs analyses au Secrétaire général et participer activement aux travaux des forums internationaux consacrés à la cybersécurité et à ceux des instances interrégionales. Grâce à la mise en commun des bonnes pratiques et des expériences, les États pourront être mieux à même de s'adapter à des normes en constant évolution et agir de manière responsable dans le cyberespace.

Il incombe à tous les États de défendre la paix et la sécurité internationale, en ligne aussi bien que hors ligne. Le meilleur point de départ est d'observer les normes de comportement responsable des États et les obligations que le droit international fait à ces derniers.