Nations Unies A/78/265

Assemblée générale

Distr. générale
1er août 2023
Français
Original : anglais

Soixante-dix-huitième session
Point 96 de l'ordre du jour provisoire*
Progrès de l'informatique et des télécommunications et sécurité internationale

Progrès de l'informatique et des télécommunications et sécurité internationale

Note du Secrétaire général

Le Secrétaire général a l'honneur de transmettre aux membres de l'Assemblée générale le deuxième rapport d'activité annuel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

* A/78/150.

23-14962 (F) 080923 180923

Merci de recycler

Rapport du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025)

I. Introduction

1. Dans sa résolution 75/240, l'Assemblée générale a décidé, pour veiller à ce que le processus de négociation démocratique, inclusif et transparent sur la sécurité d'utilisation du numérique se poursuive de manière ininterrompue, de constituer, à partir de 2021 et sous l'égide de l'Organisation des Nations Unies, un nouveau groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) qui serait chargé, sur la base du consensus : de poursuivre l'élaboration, à titre prioritaire, des règles, normes et principes de comportement responsable des États et de définir des moyens de les appliquer, ainsi que d'y apporter des changements ou d'en établir des nouveaux, selon qu'il conviendrait ; d'examiner les initiatives prises par les États pour assurer la sécurité d'utilisation du numérique ; d'instaurer, sous l'égide de l'Organisation des Nations Unies, un dialogue institutionnel régulier fondé sur une large participation des États ; de poursuivre l'examen des risques qui se posaient ou pourraient se poser dans le domaine de la sécurité numérique, notamment en ce qui concernait la sécurité des données, et des mesures de coopération qui pourraient être prises pour les prévenir et les combattre, de la manière dont le droit international s'appliquait à l'utilisation du numérique par les États ainsi que des mesures de confiance et de renforcement des capacités, en vue de parvenir à une vision commune ; de lui présenter, pour adoption par consensus, des rapports d'activité annuels et, à sa quatre-vingtième session, un rapport final sur les résultats de ses travaux.

2. Le premier rapport d'activité annuel du groupe de travail, sur sa session d'organisation et ses première, deuxième et troisième sessions de fond, a été publié sous la cote A/77/275.

II. Questions d'organisation

A. Ouverture et durée des quatrième et cinquième sessions de fond

3. Le groupe de travail a tenu sa quatrième session de fond du 6 au 10 mars 2023, et sa cinquième session de fond du 24 au 28 juillet 2023, au Siège de l'Organisation des Nations Unies.

4. Le Bureau des affaires de désarmement et l'Institut des Nations Unies pour la recherche sur le désarmement ont apporté un appui de fond au groupe de travail. Le Département de l'Assemblée générale et de la gestion des conférences a assuré les services de secrétariat.

B. Participation

5. La liste des participantes et participants aux quatrième et cinquième sessions de fond figure dans les documents publiés sous les cotes A/AC.292/2023/INF/2 et A/AC.292/2023/INF/4, respectivement.

C. Membres du Bureau

6. À ses quatrième et cinquième sessions de fond, le groupe de travail était présidé par M. Burhan Gafoor (Singapour).

D. Organisation des travaux

7. À la 1re séance de sa quatrième session de fond, le 6 mars 2023, le groupe de travail a approuvé l'organisation de ses travaux telle qu'elle figure dans le document publié sous la cote A/AC.292/2023/2/Rev.1. Il a également approuvé la participation à ses travaux des entités non gouvernementales dont la liste figure dans le document publié sous la cote A/AC.292/2023/INF/1.

8. À la 1re séance de sa cinquième session de fond, le 24 juillet 2023, le groupe de travail a approuvé l'organisation de ses travaux telle qu'elle figure dans le document publié sous la cote A/AC.292/2023/3. Il a également approuvé la participation à ses travaux des entités non gouvernementales dont la liste figure dans le document publié sous la cote A/AC.292/2023/INF/3.

E. Documentation

9. Une liste complète de tous les documents officiels, documents de travail, documents techniques et autres documents dont a été saisi le groupe de travail est disponible sur le site Web qui lui est consacré (https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021).

F. Activités du groupe de travail

10. À sa quatrième session de fond, le groupe de travail a examiné les points 3, 5 et 6 de l'ordre du jour durant ses dix séances plénières.

11. À sa cinquième session de fond, le groupe de travail a examiné les points 3, 5 et 7 de l'ordre du jour durant ses dix séances plénières.

12. Du 5 au 9 décembre 2022, le 2 mars 2023 et du 23 au 26 mai 2023, le Président a organisé des réunions intersessions pour entendre les vues des parties prenantes sur les sujets examinés par le groupe de travail, qui figurent dans le mandat confié à celui-ci, tel que défini dans la résolution 75/240 de l'Assemblée générale, et dans son ordre du jour (A/AC.292/2021/1), et conformément à la décision 77/512 de l'Assemblée.

13. Le 9 mars et le 26 juillet 2023, conformément aux modalités de participation des parties prenantes arrêtées d'un commun accord, des débats ont été organisés avec lesdites parties durant la 8e séance de la quatrième session de fond et la 5e séance de la cinquième session de fond.

14. Le 1er mars, le 22 mai et le 11 juillet 2023, le Président a organisé des débats consultatifs avec les parties prenantes concernées, dont des entreprises, des entités non gouvernementales et des universités, afin d'entendre leurs vues sur les sujets examinés par le groupe de travail, qui figurent dans le mandat confié à celui-ci, tel que défini dans la résolution 75/240 de l'Assemblée générale, et dans son ordre du jour (A/AC.292/2021/1), et de recueillir des idées concrètes auxquelles le groupe pourrait réfléchir à l'avenir.

III. Adoption du rapport

15. À sa cinquième session de fond, le 28 juillet 2023, le groupe de travail a examiné le point 7 de l'ordre du jour, intitulé « Adoption des rapports d'activité annuels », et adopté son projet de rapport (A/AC.292/2023/L.1). Il a également décidé d'inclure dans son rapport les résultats des débats tenus au titre du point 5 de l'ordre du jour, qui figurent dans le document publié sous la cote A/AC.292/2023/CRP.1, tel que révisé oralement (voir annexe).

16. Un recueil des déclarations visant à expliquer la position des États sera publié sous la cote A/AC.292/2023/INF/5.

Annexe*

Rapport d'activité sur les débats du groupe de travail tenus au titre du point 5 de l'ordre du jour

A. Vue d'ensemble

1. Les quatrième et cinquième sessions officielles ainsi que les réunions intersessions informelles du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) ont été tenues dans un environnement géopolitique toujours difficile, marqué par des préoccupations croissantes concernant l'utilisation malveillante du numérique par des acteurs étatiques et non étatiques qui a une incidence sur la paix et la sécurité internationales.

2. À ces sessions, les États ont rappelé les décisions et résolutions de consensus de l'Assemblée générale dans lesquelles ils sont convenus de s'inspirer, pour ce qui touche à l'utilisation du numérique, des rapports du groupe de travail et du Groupe d'experts gouvernementaux[1]. À cet égard, ils ont également rappelé les contributions du premier groupe de travail, créé par la résolution 73/27 de l'Assemblée générale, qui a achevé ses travaux en 2021 en adoptant son rapport final par consensus[2]. De plus, ils ont pris note du résumé établi par le Président et de la liste non exhaustive de propositions qui y était annexée, et rappelé les contributions du sixième Groupe d'experts gouvernementaux, créé en application de la résolution 73/266 de l'Assemblée générale, qui a achevé ses travaux en 2021 en adoptant son rapport final par consensus[3].

3. En outre, les États ont réaffirmé le premier rapport d'activité annuel de l'actuel groupe de travail, adopté par consensus[4], le rapport de consensus adopté en 2021 par le groupe de travail sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale ainsi que les rapports de consensus adoptés par les Groupes d'experts gouvernementaux en 2010, 2013, 2015 et 2021[5]. Ils ont rappelé que, dans leurs rapports, ces groupes avaient recommandé 11 normes facultatives et non contraignantes de comportement responsable des États et pris en considération le fait que des normes supplémentaires pourraient être élaborées au fil du temps, et réaffirmé que des mesures spécifiques de confiance, de renforcement des capacités et de coopération avaient été recommandées. Ils ont par ailleurs réaffirmé que le droit international, en particulier la Charte des Nations Unies, était applicable et essentiel pour maintenir la paix, la sécurité et la stabilité dans l'environnement numérique[6]. Ces éléments consolident le cadre cumulatif et évolutif[7] de comportement responsable des États en matière d'utilisation du numérique, qui constitue la base sur laquelle s'appuie le groupe de travail actuel.

4. Le groupe de travail a rappelé que, conformément à la résolution 75/240 de l'Assemblée générale, il avait pour mandat, sur la base du consensus : de poursuivre l'élaboration, à titre prioritaire, des règles, normes et principes de comportement responsable des États et de définir des moyens de les appliquer, ainsi que d'y apporter

---

* La version originale du présent document n'a pas été revue par les services d'édition.

[1] Décisions 75/564 et 77/512 et résolutions 70/237 et 76/19 de l'Assemblée générale.

[2] A/75/816.

[3] A/76/135.

[4] A/77/275.

[5] A/65/201, A/68/98, A/70/174 et A/76/135.

[6] Rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 7.

[7] Rapport de 2021 du Groupe d'experts gouvernementaux, A/76/135, par. 2, et résolution 76/19 de l'Assemblée générale, adoptée par consensus.

des changements ou d'en établir des nouveaux, selon qu'il conviendrait ; d'examiner les initiatives prises par les États pour assurer la sécurité d'utilisation du numérique ; d'instaurer, sous l'égide de l'Organisation des Nations Unies, un dialogue institutionnel régulier fondé sur une large participation des États ; de poursuivre l'examen des risques qui se posaient ou pourraient se poser dans le domaine de la sécurité numérique, notamment en ce qui concernait la sécurité des données, et des mesures de coopération qui pourraient être prises pour les prévenir et les combattre, de la manière dont le droit international s'appliquait à l'utilisation du numérique par les États ainsi que des mesures de confiance et de renforcement des capacités, en vue de parvenir à une vision commune ; de présenter à l'Assemblée, pour adoption par consensus, des rapports d'activité annuels et, à sa quatre-vingtième session, un rapport final sur les résultats de ses travaux. À cet égard, le groupe de travail était conscient qu'il importait de mettre en œuvre son mandat de manière équilibrée et qu'il fallait prêter dûment attention à la fois à la définition d'une vision commune entre les États en matière de sécurité d'utilisation du numérique et à la poursuite de la mise en œuvre des engagements déjà pris.

5. Le groupe de travail a reconnu que le renforcement des capacités était une mesure de confiance importante et qu'il s'agissait d'un sujet qui recoupait tous ses domaines d'action, et qu'il était essentiel d'adopter une approche intégrée du renforcement des capacités dans le contexte de la sécurité numérique. À cet égard, il est indispensable de trouver des solutions durables, efficaces et abordables.

6. Le groupe de travail s'engage à mener avec les parties prenantes un dialogue de fond, régulier et soutenu, conformément aux modalités qui ont été arrêtées par la procédure d'approbation tacite le 22 avril 2022 et officiellement adoptées à la 1re séance de la troisième session du groupe de travail le 25 juillet 2022, et conformément au mandat qui lui a été confié dans la résolution 75/240 de l'Assemblée générale, à savoir interagir, le cas échéant, avec d'autres parties intéressées, notamment les entreprises, les organisations non gouvernementales et les milieux universitaires.

7. Le groupe de travail a déclaré que les organisations régionales et sous-régionales pourraient continuer de jouer un rôle important dans la mise en œuvre du cadre de comportement responsable des États en matière d'utilisation du numérique. En outre, les échanges régionaux, interrégionaux et interorganisations peuvent ouvrir de nouvelles perspectives en matière de collaboration, de coopération et d'apprentissage mutuel. Du fait que tous les États ne sont pas membres d'une organisation régionale et que toutes les organisations régionales ne s'intéressent pas à la question de la sécurité en matière d'utilisation du numérique, le groupe de travail a noté que les initiatives régionales étaient complémentaires de ses travaux.

8. Le groupe de travail s'est félicité du haut niveau de participation des représentantes déléguées à ses sessions et de la place importante accordée aux questions de genre dans ses discussions. Il a souligné qu'il importait de réduire la fracture numérique entre les genres et de promouvoir la participation pleine, égale et véritable des femmes aux processus décisionnels liés à l'utilisation du numérique dans le contexte de la sécurité internationale, et leur influence.

9. Ce deuxième rapport d'activité annuel comprend des actions concrètes et des mesures de coopération pour faire face aux menaces liées aux technologies de l'information et des communications (TIC) et promouvoir un environnement numérique ouvert, sûr, stable, accessible et pacifique et, à cet égard, s'appuie sur le premier rapport d'activité annuel (A/77/275), approuvé par consensus dans la décision 77/512 de l'Assemblée générale. Compte tenu du fait que le groupe de travail n'en est qu'au début de ses délibérations et que les discussions de fond se poursuivront jusqu'à l'achèvement de son mandat en 2025, il ne se veut pas un résumé

complet des débats tenus entre les États, mais vise à rendre compte des progrès concrets que le groupe a accomplis à ce jour, en s'appuyant également sur la feuille de route pour les débats figurant dans le premier rapport. Il sera présenté à l'Assemblée générale conformément au mandat du groupe de travail défini dans la résolution 75/240.

B. Menaces existantes et potentielles

10. Au cours des quatrième et cinquième sessions ainsi que des sessions informelles du groupe de travail, les États ont poursuivi leurs discussions sur les menaces qui se posent ou qui pourraient se poser. À cet égard, ils ont rappelé que les travaux du groupe de travail avaient pour objet d'examiner les menaces liées au numérique dans le contexte de la sécurité internationale et ont donc entrepris des discussions sur les menaces existantes et potentielles dans cette optique spécifique. Rappelant les menaces recensées dans le premier rapport d'activité annuel du groupe de travail, dans le rapport de 2021 du groupe de travail et dans les rapports du Groupe d'experts gouvernementaux, ils ont de nouveau fait part de leur préoccupation croissante quant au fait que les menaces que l'utilisation du numérique représente pour la sécurité internationale s'intensifient et évoluent considérablement dans le contexte géopolitique actuel, qui est particulièrement complexe.

11. Les États ont rappelé qu'un certain nombre d'États développaient des capacités dans ce domaine à des fins militaires[8]. Ils ont également rappelé qu'il était de plus en plus probable que les TIC soient utilisées dans des conflits futurs entre États et ont noté qu'elles avaient déjà été utilisées dans des conflits survenus dans différentes régions. L'augmentation constante du nombre d'incidents impliquant l'utilisation malveillante des TIC par des acteurs étatiques et non étatiques, y compris des terroristes et des groupes criminels, était une tendance inquiétante. Certains acteurs non étatiques avaient montré qu'ils possédaient des capacités en matière de TIC qui n'étaient auparavant accessibles qu'aux États[9].

12. Les États se sont en outre déclarés particulièrement préoccupés par l'augmentation des activités malveillantes liées aux TIC ayant une incidence sur les infrastructures critiques et les infrastructures d'information critiques, notamment celles qui fournissent des services essentiels au-delà des frontières et des juridictions, ce qui peut avoir des effets en cascade aux niveaux national, régional et mondial, ainsi que des activités malveillantes liées aux TIC qui prennent pour cible les organisations humanitaires. Ils ont en particulier souligné l'incidence des menaces liées aux TIC sur de multiples secteurs, notamment la santé, le secteur maritime, l'aviation et l'énergie.

13. Les États ont également souligné que les attaques menées contre les infrastructures critiques et les infrastructures d'information critiques qui sapaient la confiance dans les processus politiques et électoraux et dans les institutions publiques ou qui avaient des répercussions sur la disponibilité ou l'intégrité d'Internet étaient également une préoccupation réelle et croissante [10]. Ils se sont déclarés particulièrement préoccupés par les activités malveillantes liées aux TIC qui visaient à s'immiscer dans les affaires intérieures des États.

14. En outre, des États ont noté avec préoccupation que certains États se livraient de plus en plus à des campagnes d'information clandestines facilitées par les technologies numériques en vue d'influencer les procédures, les systèmes et la

[8] Rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 16.
[9] Idem.
[10] Rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 18.

stabilité générale d'autres États. Ces activités minent la confiance, comportent un risque d'escalade et peuvent menacer la paix et la sécurité internationales. Elles peuvent également causer des dommages directs et indirects aux personnes[11].

15. Les États se sont également déclarés préoccupés par l'exploitation des vulnérabilités des produits numériques et par l'utilisation de fonctionnalités cachées néfastes, en particulier lorsque ces questions ont une incidence sur la paix et la sécurité internationales. Ils ont également souligné la menace importante qui pesait sur l'intégrité des chaînes d'approvisionnement, ainsi que le risque que posaient les logiciels malveillants tels que les logiciels rançonneurs, les logiciels de type wiper et les chevaux de Troie et les techniques telles que l'hameçonnage et les attaques par déni de service distribué.

16. Les États se sont par ailleurs déclarés préoccupés par l'utilisation irresponsable et potentiellement malveillante, y compris par les États, des capacités disponibles en matière de technologies numériques. Ils ont également exprimé leur inquiétude quant à l'utilisation des outils numériques par des acteurs malveillants.

17. Les États ont noté que les technologies nouvelles élargissaient les possibilités de développement. Toutefois, leurs propriétés et caractéristiques en constante évolution étendaient également les surfaces d'attaques, en créant de nouveaux vecteurs et des vulnérabilités qui pouvaient être exploitées aux fins d'activités malveillantes liées au numérique[12], ce qui pourrait avoir des implications sur l'utilisation des TIC dans le contexte de la sécurité internationale. Compte tenu de l'augmentation du volume de données associées aux technologies nouvelles et émergentes et de leur agrégation, les États ont également noté qu'il importait de plus en plus de protéger et de sécuriser les données. Ils ont noté avec préoccupation qu'il était devenu très difficile de veiller à ce que les vulnérabilités des technologies opérationnelles et des dispositifs, plateformes, machines ou objets informatiques interconnectés qui constituent l'Internet des objets ne soient pas exploitées à des fins malveillantes.

18. Les États ont également attiré l'attention sur la nécessité de prendre en compte les questions de genre dans la lutte contre les menaces liées aux TIC et sur les risques spécifiques auxquels sont confrontées les personnes en situation de vulnérabilité. Ils ont continué à souligner que les avantages de la technologie numérique n'étaient pas les mêmes pour tous et ont donc insisté sur la nécessité d'accorder l'attention voulue à la fracture numérique croissante dans le contexte de l'accélération de la mise en œuvre des objectifs de développement durable, tout en respectant les besoins et les priorités nationaux des États.

19. Les États ont rappelé que toute utilisation des TIC par les États d'une manière incompatible avec les obligations qui leur incombent en vertu du cadre établi pour un comportement responsable en matière d'utilisation du numérique, qui comprend des normes facultatives, le droit international et des mesures de confiance, compromettait la paix et la sécurité internationales ainsi que la confiance et la stabilité entre les États[13].

20. Les États se sont dits préoccupés par le fait qu'un manque d'information et de capacités s'agissant de détecter les attaques informatiques, de s'en défendre ou d'y

---

[11] Rapport de 2021 du Groupe d'experts gouvernementaux, A/76/135, par. 9 ; résolution 76/19 de l'Assemblée générale, adoptée par consensus.

[12] Premier rapport d'activité annuel du groupe de travail, A/77/275, par. 11 ; rapport de 2021 du Groupe d'experts gouvernementaux, A/76/135, par. 11 ; résolution 76/19 de l'Assemblée générale, adoptée par consensus.

[13] Premier rapport d'activité annuel du groupe de travail, A/77/275, par. 12 ; rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 17.

répondre pouvait les rendre plus vulnérables[14]. Compte tenu de l'évolution des menaces que représente l'utilisation des TIC, et conscients qu'aucun d'eux n'est à l'abri, ils ont souligné qu'il était urgent de fournir davantage d'informations sur ces menaces et d'en approfondir la compréhension, ainsi que de poursuivre l'élaboration et la mise en œuvre de mesures de coopération et d'initiatives de renforcement des capacités dans le cadre cumulatif et évolutif établi aux fins du comportement responsable des États[15].

Prochaines étapes recommandées

21. **Les États poursuivent, dans le cadre du groupe de travail, les échanges de vues sur les menaces que l'utilisation du numérique pose ou pourrait poser pour la sécurité et qui représentent un risque pour la paix et la sécurité internationales, ainsi que sur les mesures de coopération qui pourraient être prises pour y parer. À cet égard, ils reconnaissent que tous les États s'engagent à respecter et réaffirment l'observation et la mise en œuvre du cadre pour un comportement responsable des États en matière d'utilisation du numérique, qui reste essentiel pour faire face aux menaces informatiques qui pèsent ou pourraient peser sur la sécurité internationale.**

22. **Le groupe de travail organise également une réunion intersessions consacrée aux menaces que l'utilisation du numérique fait peser ou pourrait faire peser sur la sécurité, avec la participation d'expert(e)s compétent(e)s invité(e)s par le Président du groupe et en tenant dûment compte d'une représentation géographique équitable.**

C. Règles, normes et principes relatifs au comportement responsable des États

23. Au cours des quatrième et cinquième sessions ainsi que des sessions informelles du groupe de travail, les États ont poursuivi leurs débats sur les règles, normes et principes d'un comportement responsable de leur part. Les États, réaffirmant le cadre cumulatif et évolutif de comportement responsable des États en matière d'utilisation du numérique, ont fait des propositions concrètes et orientées vers l'action au sujet des règles, normes et principes y relatifs. On trouvera ci-après une liste non exhaustive de propositions soutenues à divers degrés par les États et susceptibles d'être étoffées et complétées lors des prochaines sessions du groupe de travail :

a) Les États ont rappelé que, conformément à la résolution 75/240 de l'Assemblée générale, le groupe de travail avait pour mandat de poursuivre l'élaboration, à titre prioritaire, des règles, normes et principes de comportement responsable des États et de définir des moyens de les appliquer, ainsi que d'y apporter des changements ou d'en établir des nouveaux, selon qu'il conviendrait[16] ;

b) Les normes facultatives et non contraignantes de comportement responsable des États peuvent permettre de réduire les risques pour la paix, la sécurité et la stabilité internationales, et jouer un rôle important pour ce qui est d'accroître la prévisibilité et de réduire le risque d'erreurs d'interprétation, contribuant ainsi à la prévention des conflits. Les États ont souligné que ces normes reflétaient les attentes et les exigences de la communauté internationale s'agissant de l'utilisation du

[14] Rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 20.
[15] Ibid., par. 22.
[16] Résolution 75/240 de l'Assemblée générale, par. 1.

numérique par les États, et qu'elles permettaient à la communauté internationale d'évaluer les activités des États[17] ;

c) Les États ont souligné qu'il fallait protéger les infrastructures critiques et les infrastructures d'information critiques. Ils ont souligné que toute activité numérique qui endommageait intentionnellement une infrastructure critique ou une infrastructure d'information critique ou qui compromettait l'utilisation et le fonctionnement de telles infrastructures fournissant des services au public pouvait avoir des répercussions en cascade aux niveaux national, régional et mondial, présentait un risque élevé de préjudice pour la population et pouvait entraîner une escalade[18]. Ils ont donc fait valoir qu'il était nécessaire de continuer à renforcer les mesures visant à protéger toutes les infrastructures critiques et les infrastructures d'information critiques contre les menaces liées aux TIC et ont proposé d'intensifier les échanges sur les meilleures pratiques à adopter pour protéger ces infrastructures, y compris le partage des politiques nationales, et pour se relever après des incidents informatiques touchant ces infrastructures. À cet égard, ils ont rappelé la résolution 58/199 de l'Assemblée générale, qui porte sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information, et son annexe[19]. Des États ont également proposé d'aider les pays en développement et les petits États à recenser leurs infrastructures critiques et leurs infrastructures d'information critiques nationales, le cas échéant ;

d) Les États ont continué à souligner que la coopération et l'assistance pouvaient être renforcées pour garantir l'intégrité des chaînes d'approvisionnement et empêcher l'utilisation de fonctionnalités cachées néfastes. Parmi les mesures raisonnables permettant de promouvoir l'ouverture et de garantir l'intégrité, la stabilité et la sécurité de ces chaînes, citons : la mise en place de politiques et de programmes visant à encourager objectivement les fournisseurs d'équipements et de systèmes numériques ainsi que les prestataires spécialisés dans ce domaine à adopter de bonnes pratiques, le but étant de renforcer la confiance dans l'intégrité et la sécurité des produits et services numériques, d'améliorer la qualité et de promouvoir le choix, ainsi que la mise en place de mesures de coopération comme la mise en commun des bonnes pratiques de gestion des risques associés à la chaîne d'approvisionnement ; l'élaboration et la mise en œuvre de règles et de normes communes en matière de sécurité de la chaîne d'approvisionnement qui soient interopérables à l'échelle mondiale ; le recours à d'autres stratégies de réduction des faiblesses de la chaîne d'approvisionnement ;

e) Les États ont noté le rôle crucial que le secteur privé jouait pour promouvoir l'ouverture et assurer l'intégrité, la stabilité et la sécurité de la chaîne d'approvisionnement et pour prévenir la prolifération des techniques et des outils numériques malveillants ainsi que l'utilisation de fonctionnalités cachées néfastes. Il a été proposé qu'en plus des étapes et des mesures décrites ci-dessus, les États continuent à renforcer leur partenariat avec le secteur privé afin d'œuvrer de concert à l'amélioration de la sécurité numérique et de l'utilisation des TIC. Les États devraient également continuer à encourager le secteur privé à jouer un rôle approprié pour améliorer la sécurité des technologies numériques et de leur utilisation, notamment en ce qui concerne la sécurité de la chaîne d'approvisionnement des produits numériques, conformément aux lois et réglementations nationales des pays dans lesquels il opère ;

---

[17] Rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 64 et 65.

[18] Rapport de 2021 du Groupe d'experts gouvernementaux, A/76/135, par. 42 ; résolution 76/19 de l'Assemblée générale, adoptée par consensus.

[19] Rapport de 2021 du Groupe d'experts gouvernementaux, A/76/135, par. 48 ; résolution 76/19 de l'Assemblée générale, adoptée par consensus.

f) Les États ont souligné la nécessité d'aider davantage les États à mettre en œuvre les règles, normes et principes d'un comportement responsable en matière d'utilisation du numérique. Il a été proposé que les États envisagent :

i) De mener, à titre volontaire, des études sur les mesures prises au niveau national pour appliquer les règles, normes et principes de comportement responsable, ainsi que sur les besoins en matière de renforcement des capacités à cet égard. Les États pourraient partager ces études dans le cadre du rapport du Secrétaire général sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et de l'enquête nationale sur la mise en œuvre, conformément aux recommandations figurant dans le rapport de 2021 du groupe de travail[20] ;

ii) De participer, à titre volontaire, à l'élaboration et à l'utilisation de nouvelles orientations ou de listes de contrôle sur la mise en œuvre des normes, en s'appuyant sur les conclusions et les recommandations adoptées dans les précédents rapports du groupe de travail et du Groupe d'experts gouvernementaux ;

g) Les États ont souligné la nécessité de poursuivre des discussions ciblées sur les règles, normes et principes d'un comportement responsable en matière d'utilisation du numérique ;

h) En ce qui concerne l'examen des propositions faites au titre de ce sujet, les États ont proposé de continuer de discuter de la liste non exhaustive des propositions formulées concernant l'enrichissement des règles, normes et principes de comportement responsable des États (annexée au résumé établi par le Président dans le rapport de 2021 du groupe de travail[21]) à la suite de la recommandation figurant dans le rapport de 2021[22].

Prochaines étapes recommandées

24. **Dans le cadre du groupe de travail, les États poursuivent, aux sixième, septième et huitième sessions du groupe, les échanges de vues sur les règles, normes et principes d'un comportement responsable en matière d'utilisation du numérique, en tenant compte des alinéas a) à h) du paragraphe 23 ci-dessus.**

25. **Aux sixième, septième et huitième sessions du groupe de travail, les États entreprennent également des discussions ciblées sur : a) le renforcement des mesures visant à protéger les infrastructures critiques et les infrastructures d'information critiques contre les menaces liées aux TIC, y compris les échanges sur les meilleures pratiques permettant de détecter les incidents informatiques, de s'en défendre, d'y répondre et de s'en relever, et à aider les pays en développement et les petits États à recenser les infrastructures critiques et les infrastructures d'information critiques au niveau national, le cas échéant ; b) la poursuite de la coopération et de l'assistance pour garantir l'intégrité des chaînes d'approvisionnement et empêcher l'utilisation de fonctionnalités cachées néfastes.**

26. **Les États élaborent des orientations supplémentaires, y compris une liste de contrôle, sur la mise en œuvre des normes, en tenant compte des accords antérieurs. Le Président du groupe de travail est invité à rédiger un premier projet de liste de contrôle pour examen par les États.**

[20] Rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 64 et 65.
[21] Rapport de 2021 du groupe de travail, A/75/816, annexe II.
[22] Rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 33.

27. **Le Président du groupe de travail est prié de convoquer une réunion intersessions spécifique pour poursuivre l'examen des règles, normes et principes relatifs au comportement responsable des États en matière d'utilisation du numérique, en tenant compte des alinéas a) à h) du paragraphe 23 ci-dessus. À cet égard, il pourrait inviter, en garantissant une représentation géographique équitable, des expert(e)s compétent(e)s issu(e)s d'organisations régionales et sous-régionales, d'entreprises, d'organisations non gouvernementales et d'universités à présenter des exposés lors de ces discussions.**

D. Droit international

28. Au cours des quatrième et cinquième sessions ainsi que des sessions informelles du groupe de travail, les États, réaffirmant le cadre cumulatif et évolutif de comportement responsable des États en matière d'utilisation du numérique, et réaffirmant en outre que le droit international, en particulier la Charte des Nations Unies, est applicable et essentiel au maintien de la paix, de la sécurité et de la stabilité et à la promotion d'un environnement numérique ouvert, sûr, stable, accessible et pacifique, ont poursuivi les discussions sur la manière dont le droit international s'appliquait à l'utilisation du numérique. Le groupe de travail a tenu des discussions ciblées et approfondies sur des sujets énumérés dans la liste non exhaustive figurant aux alinéas a) et b) du paragraphe 15 du premier rapport d'activité annuel ainsi que sur les propositions figurant dans le rapport de 2021 du groupe de travail et le résumé établi par le Président, le cas échéant[23].

29. Dans le cadre de ces discussions ciblées, les États ont été guidés par la recommandation formulée dans le premier rapport d'activité annuel selon laquelle ils devaient engager des discussions ciblées sur les sujets énumérés dans la liste non exhaustive figurant aux paragraphes suivants[24] :

a) « Le groupe de travail pourrait organiser des discussions sur des questions spécifiques relatives au droit international. Ces discussions devraient avoir pour objectif principal de recenser les domaines de convergence et de consensus. La liste non exhaustive et ouverte de sujets en lien avec le droit international que les États proposent d'examiner plus profondément comprend : la façon dont le droit international, en particulier la Charte des Nations Unies, s'applique à l'utilisation du numérique ; la souveraineté ; l'égalité souveraine ; la non-intervention dans les affaires intérieures d'autres États ; le règlement pacifique des différends ; la responsabilité des États et le devoir de précaution ; le respect des droits humains et des libertés fondamentales ; les éventuelles lacunes dans la compréhension commune de la manière dont le droit international s'applique ; les propositions figurant dans le rapport de 2021 du groupe de travail et le résumé établi par le Président, le cas échéant » ;

b) Le groupe de travail a pris note des recommandations figurant dans les rapports adoptés en 2021 par le groupe de travail précédent et par le Groupe d'experts gouvernementaux, qui se lisaient comme suit :

i) « Les États ont participé de manière régulière et active à l'ensemble des travaux du groupe de travail et les échanges de vues ont donc été extrêmement enrichissants. La valeur de ces échanges tient en partie au fait que des points de vue divers, des idées nouvelles et des propositions importantes, y compris la

[23] Premier rapport d'activité annuel du groupe de travail, A/77/275, section relative au droit international, prochaines étapes recommandées, par. 2.

[24] Premier rapport d'activité annuel du groupe de travail, A/77/275 par. 15 b) i) et ii) et section relative au droit international, prochaines étapes recommandées, par. 2.

possibilité de définir de nouvelles obligations juridiquement contraignantes, ont été mis en avant, même s'ils n'ont pas forcément fait l'unanimité parmi les États. Les différents points de vue exprimés sont reflétés dans le résumé des discussions et des formulations spécifiques proposées au titre du point de l'ordre du jour intitulé « Règles, normes et principes », qui a été établi par la présidence et joint au présent rapport. Ces éléments devraient être examinés plus avant lors de futurs processus organisés sous les auspices des Nations Unies, notamment dans le cadre des travaux du groupe de travail à composition non limitée créé en application de la résolution 75/240 de l'Assemblée générale »[25] ;

ii) « Le Groupe d'experts gouvernementaux a noté que le droit international humanitaire s'appliquait uniquement en cas de conflit armé. Il rappelle 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. Il a reconnu qu'il convenait d'examiner plus avant de quelle manière et à quel moment ces principes 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 »[26].

30. Lors des discussions ciblées du groupe de travail sur la manière dont le droit international s'applique à l'utilisation des technologies numériques, les États ont, entre autres :

a) Réaffirmé les principes de la souveraineté des États et de l'égalité souveraine ;

b) Réaffirmé le paragraphe 3 de l'Article 2 de la Charte des Nations Unies, qui dispose que tous « les Membres de l'Organisation règlent leurs différends internationaux par des moyens pacifiques, de telle manière que la paix et la sécurité internationales ainsi que la justice ne soient pas mises en danger »[27], ainsi que le paragraphe 1 de l'Article 33 de la Charte, qui dispose que « les parties à tout différend dont la prolongation est susceptible de menacer le maintien de la paix et de la sécurité internationales doivent en rechercher la solution, avant tout, par voie de négociation, d'enquête, de médiation, de conciliation, d'arbitrage, de règlement judiciaire, de recours aux organismes ou accords régionaux, ou par d'autres moyens pacifiques de leur choix »[28] ;

c) Réaffirmé le paragraphe 4 de l'Article 2 de la Charte des Nations Unies, qui dispose que tous les États Membres « s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies » ;

d) Réaffirmé en outre que, conformément au principe de non-intervention, les États n'avaient pas le droit d'intervenir directement ou indirectement dans les affaires intérieures d'un autre État, notamment au moyen des technologies numériques[29].

---

[25] Rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 80.

[26] Rapport de 2021 du Groupe d'experts gouvernementaux, A/76/135, par. 71 f) ; résolution 76/19 de l'Assemblée générale, adoptée par consensus.

[27] Paragraphe 3 de l'Article 2 de la Charte des Nations Unies.

[28] Paragraphe 1 de l'Article 33 de la Charte des Nations Unies.

[29] Rapport de 2021 du Groupe d'experts gouvernementaux, A/76/135, par. 71 c) ; résolution 76/19 de l'Assemblée générale, adoptée par consensus.

31. Les États ont également formulé d'autres propositions concrètes et orientées vers l'action au sujet du droit international :

a) Les États ont noté que les débats intersessions avaient approfondi et enrichi les discussions qui sont actuellement menées sur la manière dont le droit international s'applique à l'utilisation des TIC et ont proposé d'organiser des sessions supplémentaires au cours de la prochaine période intersessions du groupe de travail ;

b) Les États ont par ailleurs noté que le fait de partager leurs vues pouvait contribuer à forger une compréhension commune de la manière dont le droit international s'applique à l'utilisation des technologies numériques et ont encouragé la poursuite du partage, à titre volontaire, des vues sur le droit international, qui peut inclure des déclarations nationales et la pratique des États sur la manière dont le droit international s'applique à l'utilisation de telles technologies. En outre, les études et les avis pertinents des experts juridiques internationaux peuvent également aider les États à forger une telle compréhension commune ;

c) Reconnaissant les initiatives qui sont actuellement menées en matière de renforcement des capacités dans le domaine du droit international, les États ont en outre souligné qu'il fallait de toute urgence poursuivre ces efforts de renforcement des capacités, notamment pour veiller à ce que tous les États soient en mesure de participer sur un pied d'égalité à l'élaboration d'interprétations communes sur la manière dont le droit international s'applique à l'utilisation des technologies numériques. Ces efforts de renforcement des capacités pourraient inclure des ateliers, des cours de formation, des échanges sur les meilleures pratiques aux niveaux international, interrégional, régional et sous-régional, et s'inspirer de l'expérience des organisations régionales concernées, le cas échéant, et devraient être entrepris conformément aux principes de renforcement des capacités énoncés au paragraphe 56 du rapport de 2021 du groupe de travail.

32. Notant la possibilité d'établir, à l'avenir, de nouvelles obligations contraignantes, selon qu'il convient, les États ont discuté de la nécessité d'examiner les éventuelles lacunes dans la manière dont le droit international existant s'applique à l'utilisation des technologies numériques et d'envisager plus avant l'élaboration de nouvelles obligations juridiquement contraignantes[30].

Prochaines étapes recommandées

33. **Les États continuent, dans le cadre du groupe de travail, de mener des discussions ciblées sur la manière dont le droit international s'applique à l'utilisation des technologies numériques, en s'inspirant des sujets énumérés dans la liste non exhaustive figurant aux alinéas a) et b) du paragraphe 29 ci-dessus, ainsi que des propositions faites sur le thème du droit international figurant dans le rapport de 2021 du groupe de travail et dans le résumé établi par le Président, le cas échéant.**

34. **Sur la base des discussions menées aux quatrième et cinquième sessions du groupe de travail, les États sont invités à continuer, à titre volontaire, de partager leurs vues, qui peuvent inclure des déclarations nationales et la pratique des États, sur la manière dont le droit international s'applique à l'utilisation des technologies numériques. Le Secrétariat de l'ONU est prié de publier ces vues sur le site Web du groupe de travail, à l'intention de tous les États, et de permettre au groupe d'en débattre à ses sixième, septième et huitième sessions.**

35. **Le Président du groupe de travail est également invité à organiser une réunion intersessions consacrée à la manière dont le droit international**

[30] Une proposition a été faite à cet égard, comme le montre l'annexe D.

s'applique à l'utilisation du numérique. À cet égard, il pourrait organiser des réunions d'experts sur ce sujet, en tenant dûment compte d'une représentation géographique équitable et des contextes nationaux.

36. **Les États qui sont en mesure de le faire continuent de soutenir, de manière neutre et objective, les efforts supplémentaires déployés, notamment au sein du système des Nations Unies, pour renforcer les capacités dans le domaine du droit international afin que tous les États contribuent à forger une compréhension commune de la manière dont le droit international s'applique à l'utilisation des technologies numériques, et contribuer à l'instauration d'un consensus au sein de la communauté internationale. Il convient d'entreprendre ces efforts de renforcement des capacités conformément aux principes de renforcement des capacités énoncés au paragraphe 56 du rapport de 2021 du groupe de travail.**

E. Mesures de confiance

37. Au cours des quatrième et cinquième sessions ainsi que des sessions informelles du groupe de travail, les États ont poursuivi leurs discussions sur les mesures de confiance. Les États, réaffirmant le cadre cumulatif et évolutif de comportement responsable des États en matière d'utilisation du numérique, ont fait des propositions concrètes et orientées vers l'action au sujet des mesures de confiance. On trouvera ci-après une liste non exhaustive de propositions soutenues à divers degrés par les États et susceptibles d'être étoffées et complétées lors des prochaines sessions du groupe de travail :

a) Rappelant qu'ils étaient convenus, dans le cadre du premier rapport d'activité annuel, d'établir, en s'appuyant sur les travaux déjà accomplis au niveau régional, un répertoire mondial et intergouvernemental d'interlocuteurs[31], les États ont proposé que le groupe de travail décide d'adopter le document intitulé « Éléments concernant l'élaboration et la mise en service d'un répertoire mondial et intergouvernemental d'interlocuteurs », qui figure à l'annexe A du présent rapport, en tant que prochaine étape de la mise en service du répertoire mondial d'interlocuteurs ;

b) Les États ont reconnu que l'élaboration et la mise en service du répertoire mondial d'interlocuteurs constituaient une étape importante dans l'instauration d'un climat de confiance entre les États au niveau mondial. Ils ont en outre reconnu que le répertoire pouvait faciliter la mise en œuvre, à l'échelle mondiale, d'autres mesures de confiance qui pourraient contribuer à promouvoir un environnement numérique ouvert, sûr, stable, accessible et pacifique. À cet égard, rappelant les recommandations relatives aux mesures de confiance qui figurent dans les rapports de consensus, ils ont proposé qu'une première liste de mesures de confiance volontaires et mondiales soit établie à partir de ces rapports en vue de leur mise en œuvre par les États, y compris par l'intermédiaire du répertoire ;

c) Outre les mesures de confiance déjà approuvées dans les précédents rapports des Nations Unies, les États ont également proposé des mesures supplémentaires qui pourraient, à terme, être reconnues comme des mesures de confiance supplémentaires au niveau mondial. Il s'agit notamment des éléments suivants pour les mesures de confiance qui s'appuient sur le répertoire mondial d'interlocuteurs, sachant que toutes ces propositions ont également été incluses en

[31] Premier rapport d'activité annuel du groupe de travail, A/77/275, section relative aux mesures de confiance, prochaines étapes recommandées, par. 2.

tant qu'éléments opérationnels dans le document figurant à l'annexe A du présent rapport :

i) Contrôles de communication sous forme de tests « ping » ;

ii) Partage volontaire d'informations, notamment en cas d'incident informatique majeur ou urgent, facilité par le répertoire mondial d'interlocuteurs ;

iii) Exercices de simulation visant à simuler les aspects pratiques de la participation à un répertoire mondial d'interlocuteurs ;

iv) Réunions régulières des interlocuteurs, en ligne ou en présentiel, visant à partager des informations pratiques et des expériences sur la mise en service et l'utilisation du répertoire mondial sur une base volontaire ;

d) Les États ont souligné qu'il importait de faire en sorte que les vulnérabilités numériques soient corrigées rapidement afin de limiter les risques qu'elles ne soient exploitées par des individus mal intentionnés. La détection rapide ainsi que la divulgation et le signalement responsables et objectifs de ces vulnérabilités peuvent prévenir des pratiques néfastes ou dangereuses, renforcer la confiance et réduire les menaces connexes qu'elles font peser sur la sécurité et la stabilité internationales[32]. Il a été proposé que cette question soit examinée plus avant au sein du groupe de travail ;

e) Les États ont suggéré que le fait de partager leurs vues sur les termes techniques relatifs aux TIC pouvait améliorer la transparence et renforcer la compréhension entre les États ;

f) Il a été proposé que les activités de renforcement de la confiance continuent de prendre notamment la forme d'un dialogue avec les organisations régionales et sous-régionales et les parties prenantes intéressées, notamment les entreprises, les organisations non gouvernementales et les universités, selon qu'il convient ;

g) Les États ont souligné une fois de plus que le groupe de travail lui-même servait de mécanisme de renforcement de la confiance, en fournissant un forum permettant de discuter des questions sur lesquelles il existe un accord et des questions sur lesquelles il n'y en a pas encore.

Prochaines étapes recommandées

38. **Les États poursuivent, au sein du groupe de travail, les échanges de vues sur l'élaboration et la mise en œuvre des mesures de confiance, notamment sur la possibilité de définir des mesures de confiance supplémentaires.**

39. **Rappelant qu'ils étaient, dans le premier rapport d'activité annuel du groupe de travail, convenus d'établir un répertoire mondial et intergouvernemental d'interlocuteurs[33], les États conviennent en outre d'adopter le document intitulé « Éléments concernant l'élaboration et la mise en service d'un répertoire mondial et intergouvernemental d'interlocuteurs », qui figure à l'annexe A du présent rapport, comme prochaine étape de la mise en service du répertoire.**

[32] Rapport de 2021 du Groupe d'experts gouvernementaux, A/76/135, par. 60 ; résolution 76/19 de l'Assemblée générale, adoptée par consensus.

[33] Premier rapport d'activité annuel du groupe de travail, A/77/275, section relative aux mesures de confiance, prochaines étapes recommandées, par. 2.

40. **Les États poursuivent leurs discussions et prennent part à la mise en service du répertoire mondial d'interlocuteurs lors des sixième, septième et huitième sessions du groupe de travail, y compris dans le contexte des alinéas b) et c) du paragraphe 37 du présent rapport.**

41. **Les États recommandent la liste initiale non exhaustive des mesures de confiance volontaires au niveau mondial, figurant à l'annexe B, établie à partir des mesures de confiance convenues par consensus dans le rapport de 2021 du groupe de travail et dans les premier et deuxième rapports d'activité annuels de l'actuel groupe de travail. Le Président du groupe est invité à faciliter la poursuite des discussions sur la manière d'élaborer, de compléter et de mettre en œuvre ces mesures de confiance, y compris, entre autres, grâce : a) au renforcement des capacités correspondantes ; b) au répertoire mondial d'interlocuteurs.**

42. **Les États sont encouragés à partager, à titre volontaire, leurs vues sur les termes techniques relatifs aux TIC afin d'améliorer la transparence et de renforcer la compréhension entre les États.**

F. Renforcement des capacités

43. Au cours des quatrième et cinquième sessions ainsi que des sessions informelles du groupe de travail, les États ont poursuivi leurs discussions sur le renforcement des capacités en matière de technologies numériques dans le contexte de la sécurité internationale. Réaffirmant le cadre cumulatif et évolutif de comportement responsable des États en matière d'utilisation du numérique, ils ont fait des propositions concrètes et orientées vers l'action au sujet du renforcement des capacités. On trouvera ci-après une liste non exhaustive de propositions soutenues à divers degrés par les États et susceptibles d'être étoffées et complétées lors des prochaines sessions du groupe de travail :

a) Les États ont proposé que les principes de renforcement des capacités adoptés dans le rapport 2021 du groupe de travail[34] soient davantage pris en compte dans les initiatives de renforcement des capacités menées aux fins de la sécurité dans l'utilisation des technologies numériques. En outre, ils ont continué d'encourager les activités de renforcement des capacités tenant compte des questions de genre, notamment par l'intégration des questions de genre dans les politiques nationales relatives aux TIC et au renforcement des capacités, ainsi que par l'élaboration de listes de contrôle ou de questionnaires permettant de recenser les besoins et les lacunes dans ce domaine ;

b) Les États ont souligné l'importance de la coopération Sud-Sud, de la coopération triangulaire, de la coopération sous-régionale et régionale, en complément de la coopération Nord-Sud ;

c) Le groupe de travail pourrait promouvoir une meilleure compréhension des besoins des pays en développement dans le but de réduire la fracture numérique en adaptant les efforts de renforcement des capacités, afin que tous les États aient les capacités nécessaires pour respecter et mettre en œuvre le cadre cumulatif et évolutif de comportement responsable des États en matière d'utilisation du numérique ;

d) Les États ont souligné qu'il était nécessaire de mieux coordonner les activités de renforcement des capacités menées aux fins de la sécurité numérique et que l'ONU pouvait jouer un rôle important à cet égard, notamment en faisant le point sur les besoins des États en matière de renforcement des capacités, en recensant les

[34] Rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 56.

lacunes dans ce domaine au moyen d'outils et d'enquêtes et en facilitant l'accès des États aux programmes de renforcement des capacités. Il a été proposé que le Secrétariat de l'ONU rassemble les programmes et initiatives de renforcement des capacités existants liés à la sécurité dans l'utilisation du numérique au sein et en dehors des Nations Unies et aux niveaux mondial et régional, afin de faciliter les discussions qui seront menées ultérieurement au sein du groupe de travail sur les moyens d'améliorer la synergie, la coordination et l'accès aux programmes de renforcement des capacités proposés ;

e) Tout en reconnaissant les initiatives permettant de financer les activités de renforcement des capacités en matière de sécurité de l'utilisation du numérique, les États pourraient dans le même temps continuer d'envisager des modes de financement supplémentaires spécifiquement destinés à ces activités, s'appuyant sur les possibilités de coordination et d'harmonisation avec les programmes et fonds de développement existants ;

f) Les États ont examiné l'initiative visant à mettre en place un portail mondial de coopération en matière de cybersécurité, en proposant qu'il soit pratique et neutre, qu'il soit piloté par les États Membres et qu'il constitue un outil modulaire à guichet unique pour les États, élaboré sous l'égide de l'ONU. Il a également été suggéré de créer une synergie entre ce portail et d'autres portails existants, selon qu'il convient. Les États ont en outre proposé qu'un répertoire des meilleures pratiques en matière de renforcement des capacités dans le domaine de la sécurité numérique soit intégré à l'initiative visant à mettre en place un portail mondial. À cet égard, ils ont également souligné qu'il importait de renforcer la connaissance et la compréhension des accords précédents figurant dans les rapports du groupe de travail et du Groupe d'experts gouvernementaux afin d'éclairer leurs travaux actuels ;

g) Les États ont reconnu que le groupe de travail pourrait lui-même servir de plateforme permettant de poursuivre l'échange de vues et d'idées sur les mesures de renforcement des capacités en matière de sécurité numérique, y compris sur la meilleure façon de tirer parti des initiatives existantes afin d'aider les États à se doter de la force institutionnelle nécessaire pour mettre en œuvre le cadre de comportement responsable dans ce domaine. Il a été proposé qu'ils discutent des capacités qui peuvent les aider à cet égard. Sur la base de la table ronde utile sur le renforcement des capacités que le Président du groupe de travail a organisée en mai 2023, il a également été proposé que d'autres tables rondes soient organisées sur ce sujet sous les auspices du groupe de travail, avec la participation des parties prenantes et des praticiens concernés, afin d'échanger les meilleures pratiques en matière de renforcement des capacités dans le domaine de la sécurité numérique internationale ;

h) Les États se sont dits préoccupés par le fait qu'un manque d'information et de capacités s'agissant de détecter les attaques informatiques, de s'en défendre ou d'y répondre pouvait les rendre plus vulnérables[35]. À cet égard, ils ont examiné une proposition visant à encourager la poursuite des échanges techniques sur les menaces liées aux TIC afin de renforcer leur capacité à recenser et à détecter les activités malveillantes liées aux TIC, à s'en défendre et à y répondre en connaissance de cause, en tenant compte des mécanismes existants, tels que les canaux entre équipes d'intervention informatique d'urgence, et en les complétant ;

i) Les États pourraient, notamment dans le cadre du groupe de travail, continuer de renforcer la coordination et la coopération avec les parties prenantes intéressées, dont les entreprises, les organisations non gouvernementales et les universités. Ils ont noté que les parties prenantes jouaient déjà un rôle important dans le cadre de partenariats avec les États y compris à des fins de formation et de

[35] Rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 20.

recherche. Ils ont en outre reconnu que le renforcement des capacités était également nécessaire pour identifier les parties prenantes et engager un véritable dialogue avec elles afin de renforcer l'élaboration des politiques et d'établir la confiance nécessaire pour traiter les atteintes à la sécurité numérique en coopération avec les parties prenantes.

Prochaines étapes recommandées

44. **Les États continuent, dans le cadre du groupe de travail, d'échanger leurs vues sur les initiatives de renforcement des capacités menées aux fins de la sécurité dans l'utilisation du numérique, y compris sur les alinéas a) à i) du paragraphe 43 ci-dessus. Ils poursuivent des discussions ciblées sur la manière dont lesdites initiatives peuvent davantage tenir compte des principes de renforcement des capacités adoptés dans le rapport de 2021 du groupe de travail (qui figurent à l'annexe C).**

45. **Le Président du groupe de travail est prié de prendre contact avec les entités des Nations Unies et les organisations internationales compétentes qui proposent des programmes de renforcement des capacités en matière de sécurité dans l'utilisation du numérique et de les encourager à aligner leurs programmes de renforcement des capacités, le cas échéant et conformément à leurs mandats respectifs, afin d'aider davantage les États à mettre en œuvre le cadre de comportement responsable des États en matière d'utilisation du numérique et à s'efforcer d'instaurer un environnement numérique ouvert, sûr, stable, accessible et pacifique.**

46. **Le Secrétariat de l'ONU est prié de procéder à un « état des lieux », en consultation avec les entités concernées, afin d'examiner les programmes et les initiatives de renforcement des capacités qui existent actuellement au sein et en dehors du système des Nations Unies et aux niveaux mondial et régional, y compris en sollicitant les vues des États Membres. Il est en outre prié d'établir un rapport sur les résultats de cet « état des lieux » et de le présenter à la septième session du groupe de travail afin d'aider les États à faire le point sur les activités de renforcement des capacités en matière de sécurité numérique et d'encourager de nouvelles synergies et une meilleure coordination entre ces activités.**

47. **Les États poursuivent l'examen de la proposition tendant à mettre en place un portail mondial de coopération en matière de cybersécurité en tant qu'outil à « guichet unique » pour les États, élaboré sous l'égide de l'ONU. D'autres discussions pourraient être menées sur la manière de créer une synergie entre ce portail et d'autres portails existants, selon qu'il convient.**

48. **Le Président du groupe de travail est prié d'organiser une table ronde mondiale sur le renforcement des capacités en matière de sécurité numérique entre les sessions, afin de permettre un échange d'informations et de bonnes pratiques. Cette table ronde pourrait réunir des praticiens du renforcement des capacités ainsi que des représentantes et représentants des États intéressés et des parties prenantes concernées, notamment des entreprises, des organisations non gouvernementales et des universités, compte étant dûment tenu d'une représentation géographique équitable.**

49. **Afin de renforcer la connaissance et la compréhension des accords précédents figurant dans les rapports du groupe de travail et du Groupe d'experts gouvernementaux, ce qui permettrait d'éclairer les travaux que les États mènent actuellement au sein du groupe de travail, les États en mesure de le faire sont encouragés à aider le Secrétariat de l'ONU à mettre à jour le cours**

d'apprentissage en ligne sur la cyberdiplomatie destiné aux diplomates, dans le but d'obtenir un cours actualisé en 2024. Le Secrétariat est prié de fournir aux États des informations à ce sujet à la sixième session du groupe de travail. Il est encouragé à consulter les entités concernées pour mettre le cours à jour.

50. **Les États intéressés sont encouragés à élaborer et à partager, à titre volontaire, des listes de contrôle et d'autres outils pour aider les États à intégrer les principes de renforcement des capacités énoncés dans le rapport de 2021 du groupe de travail dans les initiatives de renforcement des capacités relatives à la sécurité numérique, ainsi que des outils qui aideraient les États à intégrer les questions de genre dans ces initiatives.**

51. **Les États qui en ont la possibilité sont invités à continuer de soutenir les programmes de renforcement des capacités, y compris en collaboration, selon qu'il convient, avec les organisations régionales et sous-régionales et les autres parties prenantes intéressées, dont les entreprises, les organisations non gouvernementales et les universités.**

G. Dialogue institutionnel régulier

52. Au cours des quatrième et cinquième sessions ainsi que des sessions informelles du groupe de travail, les États ont poursuivi leurs discussions sur le dialogue institutionnel régulier. Réaffirmant le cadre cumulatif et évolutif de comportement responsable des États en matière d'utilisation du numérique, ils ont fait des propositions concrètes et orientées vers l'action au sujet du dialogue institutionnel régulier. On trouvera ci-après une liste non exhaustive de propositions soutenues à divers degrés par les États et susceptibles d'être étoffées et complétées lors des prochaines sessions du groupe de travail :

a) Les États ont continué à souligner que le groupe de travail pouvait contribuer à sensibiliser l'opinion, à instaurer la confiance et à encourager des discussions plus approfondies sur les domaines dans lesquels aucune communauté de vues ne s'est encore dégagée. En outre, le groupe de travail devrait faire fond sur les accords précédents. Les États ont reconnu le caractère central du groupe en tant que mécanisme de dialogue sur la sécurité de l'utilisation des technologies numériques au sein du système des Nations Unies[36] ;

b) Pour donner suite à la recommandation figurant dans le rapport de 2021[37] et dans le premier rapport d'activité annuel[38] du groupe de travail, les États ont approfondi les discussions sur la proposition tendant à mettre en place un programme d'action visant à promouvoir un comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. D'autres propositions ont été faites au sujet d'un dialogue institutionnel régulier, y compris une proposition visant à créer un futur groupe, comité, commission ou conférence sous l'égide de l'ONU.

53. Reconnaissant que diverses options possibles ont été suggérées pour un dialogue institutionnel régulier, il a été proposé que, dans un premier temps, pour instaurer la confiance et favoriser la convergence, les États présentent des propositions visant à recenser certains éléments communs qui pourraient étayer l'élaboration de tout futur mécanisme de dialogue institutionnel régulier sur la sécurité dans l'utilisation du

[36] Premier rapport d'activité annuel du groupe de travail, A/77/275, par. 18 a) ;
[37] Rapport de 2021 du groupe de travail, A/75/816, annexe I, par. 77.
[38] Premier rapport d'activité annuel du groupe de travail, A/77/275, section relative au dialogue institutionnel régulier, prochaines étapes recommandées, par. 2.

numérique, tout en poursuivant les discussions sur les propositions figurant aux alinéas a) et b) du paragraphe 52.

Prochaines étapes recommandées

54. **Les États poursuivent, dans le cadre du groupe de travail, les échanges de vues sur le dialogue institutionnel régulier et sur les propositions qu'ils ont formulées en vue de faciliter le dialogue institutionnel régulier sur la sécurité en matière d'utilisation des technologies numériques, l'objectif étant d'aboutir à une conception commune du meilleur format à adopter pour le dialogue institutionnel régulier, avec une large participation des États sous les auspices de l'ONU.**

55. **Les États conviennent en principe que tout futur mécanisme de dialogue institutionnel régulier sera fondé sur les éléments communs suivants et acceptent de poursuivre les discussions sur des éléments supplémentaires :**

a) Il s'agirait d'un mécanisme permanent à voie unique, dirigé par les États et placé sous l'égide de l'ONU, qui ferait rapport à la Première Commission de l'Assemblée générale ;

b) L'objectif du futur mécanisme serait de continuer à promouvoir un environnement numérique ouvert, sûr, stable, accessible, pacifique et interopérable ;

c) Le futur mécanisme s'appuierait sur les accords consensuels obtenus sur le cadre de comportement responsable des États en matière d'utilisation du numérique, issus des précédents rapports du groupe de travail et du Groupe d'experts gouvernementaux ;

d) Il s'agirait d'un processus ouvert, inclusif, transparent, durable et flexible, capable d'évoluer en fonction des besoins des États et de l'évolution de l'environnement numérique.

56. **Les États ont reconnu l'importance du principe du consensus, tant pour la mise en place du futur mécanisme que pour ses processus décisionnels.**

57. **D'autres parties intéressées, notamment les entreprises, les organisations non gouvernementales et les universités, pourraient contribuer à un futur dialogue institutionnel régulier, le cas échéant.**

58. **Aux sixième, septième et huitième sessions du groupe de travail, ainsi que lors de deux réunions intersessions spécifiques, les États continuent de mener des discussions ciblées dans le cadre du groupe de travail afin d'examiner plus avant les propositions relatives au dialogue institutionnel régulier, y compris le programme d'action. Lors de ces sessions, ils tiennent également des discussions ciblées sur la relation entre le programme d'action et le groupe de travail, ainsi que sur la portée, le contenu et la structure du programme d'action[39]. Le Secrétariat de l'ONU est également prié de présenter au groupe de travail, à sa sixième session, des informations sur le rapport du Secrétaire général présenté à l'Assemblée générale à sa soixante-dix-huitième session[40].**

59. **Les États qui sont en mesure de le faire continuent de s'employer à mettre en place ou à appuyer des programmes de parrainage et d'autres mécanismes pour assurer une large participation aux travaux de l'ONU dans ce domaine.**

---

[39] Premier rapport d'activité annuel du groupe de travail, A/77/275, section relative au dialogue institutionnel régulier, prochaines étapes recommandées, par. 2.

[40] A/78/76.

H. Observations finales

60. Les États ont pris note de la participation constructive des délégations de toutes les régions aux travaux du groupe de travail au cours des cinq dernières sessions de fond, et de leur collaboration croissante. Ils ont apporté une contribution substantielle auxdits travaux lors de ces sessions. Les États et groupes d'États ont également soumis au groupe de travail des documents de travail exposant leurs positions, idées et initiatives nationales et collectives sur les questions relevant de son mandat. Leur liste figure à l'annexe D.

Annexe A

Éléments concernant l'élaboration et la mise en service d'un répertoire mondial et intergouvernemental d'interlocuteurs

1. Conformément au premier rapport d'activité annuel du groupe de travail, publié sous la cote A/77/275, dans lequel « les États conviennent d'établir un répertoire mondial et intergouvernemental d'interlocuteurs, en s'appuyant sur les travaux déjà réalisés au niveau régional », le présent document expose les éléments qui peuvent guider l'élaboration et la mise en service d'un tel répertoire sur l'utilisation des technologies numériques dans le contexte de la paix et de la sécurité internationales.

Buts et principes

2. Un répertoire mondial et intergouvernemental d'interlocuteurs constituerait en soi une mesure de confiance et fournirait également une base pour mettre en œuvre d'autres mesures de confiance qui pourraient contribuer à promouvoir un environnement numérique ouvert, sûr, stable, accessible et pacifique.

3. Le répertoire est conçu pour être volontaire, pratique et neutre par nature, élaboré et mis en œuvre conformément aux principes de souveraineté, d'égalité souveraine, de règlement des différends par des moyens pacifiques et de non-intervention dans les affaires intérieures d'autres États.

4. Le répertoire prendra en compte les travaux des réseaux d'équipes d'intervention informatique d'urgence et d'équipes d'intervention en cas d'atteinte à la sécurité informatique, qui viendront le compléter.

5. Les principaux objectifs du répertoire sont les suivants :

a) Renforcer l'interaction et la coopération entre les États et, ce faisant, promouvoir la paix et la sécurité internationales et accroître la transparence et la prévisibilité ;

b) Faciliter la coordination et la communication entre les États, notamment en cas d'incident informatique majeur ou urgent, afin de renforcer la confiance entre les États, de réduire les tensions et d'éviter les malentendus et les méprises que risquent d'engendrer des incidents informatiques ;

c) Accroître la communication et le partage d'informations et permettre aux États, notamment par le renforcement des capacités, de faciliter la prévention et la détection des incidents informatiques majeurs ou urgents, d'y répondre et de s'en relever ;

d) Le répertoire d'interlocuteurs peut faciliter les communications sécurisées et directes entre les États dans le cadre de la prévention et de la gestion des atteintes graves à la sécurité informatique et désamorcer les tensions dans des situations de crise. La communication entre ces interlocuteurs peut contribuer à réduire les tensions et à éviter les malentendus et les méprises que risquent d'engendrer des incidents informatiques, notamment ceux qui touchent des infrastructures critiques et qui ont un impact aux niveaux national, régional et mondial. Elle peut également accroître l'échange d'informations et permettre aux États de mieux gérer et régler ces incidents[41].

[41] Rapport de 2021 du Groupe d'experts gouvernementaux, A/76/135, par. 76 ; résolution 76/19 de l'Assemblée générale, adoptée par consensus.

Modalités

6. **Accès et participation**. La participation au répertoire, y compris la présentation d'informations, se ferait à titre volontaire. Les États souhaitant participer au répertoire s'en verront accorder l'accès.

7. **Spécifications du répertoire**. Le Bureau des affaires de désarmement de l'ONU serait le gestionnaire du répertoire et serait chargé de développer et de rendre opérationnels les aspects techniques du répertoire conformément aux spécifications suivantes :

a) Schéma d'information :

i) Les États peuvent désigner, dans la mesure du possible, des interlocuteurs diplomatiques et techniques pour le répertoire ;

ii) Les États peuvent désigner comme interlocuteurs soit une entité/institution nationale autorisée, soit un(e) représentant(e) désigné(e) spécifique d'une entité/institution nationale autorisée ;

iii) Les États peuvent fournir des informations sur l'entité/institution, des coordonnées (numéro de téléphone et adresse électronique), le nom et la désignation de l'interlocuteur (le cas échéant), et sa ou ses langues de travail ;

iv) Chaque entrée dans le répertoire peut être présentée dans n'importe quelle langue officielle de l'ONU ; en outre, la présentation d'une traduction anglaise non officielle est encouragée ;

b) Protection de l'information : le répertoire sera hébergé en ligne sur un site Web sécurisé. Il n'hébergera pas d'informations confidentielles transmises ou échangées entre les interlocuteurs. Ces derniers communiqueront et échangeront des informations confidentielles grâce à des canaux convenus d'un commun accord, notamment des canaux sécurisés le cas échéant ;

c) Accès à l'information : les États peuvent demander au Bureau des affaires de désarmement, par l'intermédiaire de leur mission permanente à New York, des identifiants de connexion au site Web. À des fins d'information générale, une page publique présentant une vue d'ensemble du mandat du répertoire serait disponible sur le site Web du Bureau ;

d) Gestion de l'information : les États peuvent progressivement mettre à jour les informations figurant dans le répertoire si celles qu'ils ont communiquées venaient à connaître des modifications.

8. **Mise à jour du répertoire**. Le gestionnaire du répertoire doit effectuer des tests « ping » tous les six mois pour vérifier que les informations qui y figurent sont à jour. Dans le cadre desdits tests, il contactera les interlocuteurs listés dans le répertoire, qui devront répondre dans un délai de 48 heures et confirmer par message qu'ils ont bien reçu la demande du gestionnaire. En l'absence de réponse au test « ping », il s'efforcera de contacter les autorités compétentes de l'État concerné pour les encourager à mettre à jour leurs informations.

9. **Rôles des interlocuteurs diplomatiques et techniques**. Il est prévu que les interlocuteurs diplomatiques et techniques aient des rôles différenciés. Les interlocuteurs diplomatiques communiqueront ainsi avec d'autres interlocuteurs diplomatiques et les interlocuteurs techniques avec d'autres interlocuteurs techniques. La coordination entre les interlocuteurs d'un même État est encouragée. Les États peuvent prendre en considération les fonctions suggérées ci-dessous lorsqu'ils définissent les rôles de leurs interlocuteurs conformément à leurs politiques et législations nationales.

a) Les interlocuteurs diplomatiques peuvent établir une communication avec d'autres interlocuteurs diplomatiques, notamment en cas d'incident informatique majeur ou urgent, dans le but de prévenir les malentendus et de réduire les tensions. Si nécessaire, ils peuvent envisager de porter l'incident à l'attention de fonctionnaires de haut niveau, au sein de leurs structures gouvernementales nationales respectives, afin qu'une communication plus poussée puisse avoir lieu entre les États, selon qu'il convient. Le cas échéant, ils peuvent être issus d'une agence nationale autorisée chargée de la coopération internationale ;

b) Les interlocuteurs techniques peuvent établir une communication avec d'autres interlocuteurs techniques, notamment en cas d'incident informatique majeur ou urgent, dans le but de fournir ou de demander des informations ou de l'aide. Une telle communication peut notamment prendre la forme d'une demande d'information ou d'une demande d'action ou d'assistance spécifique. Les interlocuteurs techniques peuvent également, à titre volontaire, échanger avec d'autres interlocuteurs techniques les meilleures pratiques, les enseignements tirés et d'autres informations pertinentes sur la manière de faciliter la prévention et la détection, entre autres, des incidents informatiques majeurs ou urgents, d'y répondre et de s'en relever. Le cas échéant, les interlocuteurs techniques peuvent être des agences nationales autorisées qui travaillent sur la sécurité numérique et qui sont responsables de la prévention et de la détection des incidents informatiques, de la réponse qui y est apportée et du relèvement, comme l'équipe nationale d'intervention informatique d'urgence ou l'équipe nationale d'intervention en cas d'atteinte à la sécurité informatique.

10. **Interaction entre les interlocuteurs**. Il appartient à chaque État de déterminer la manière de répondre aux communications reçues via le répertoire. Toute information est échangée à titre volontaire et est conforme aux différentes circonstances, exigences et législations nationales des États concernés. Toute coopération ou tout partage d'informations ultérieurs, y compris le canal par lequel la communication pertinente aurait lieu, se dérouleraient conformément à l'accord mutuel passé. Le fait d'accuser réception d'une communication ne revient pas à approuver les informations qu'elle contient ni ne préjuge de la position de l'État répondant, pas plus qu'il ne préjuge de toute communication qui pourrait s'ensuivre. De plus, le fait d'informer un État que son territoire est utilisé pour un acte illicite n'implique pas, en soi, que cet État est responsable de l'acte[42].

a) Les interlocuteurs peuvent souhaiter utiliser des procédures standardisées lorsqu'ils interagissent avec d'autres interlocuteurs. Dans un premier temps, pour faciliter la communication, ils peuvent envisager d'utiliser, à titre volontaire, la « Procédure de demande de renseignements » et la « Procédure de réponse à une demande de renseignements » figurant à l'appendice de la présente pièce jointe ;

b) Les interlocuteurs peuvent également souhaiter utiliser des modèles standardisés lorsqu'ils interagissent avec d'autres interlocuteurs. Ces modèles standardisés peuvent préciser les types d'informations à fournir au moment de communiquer, y compris les données techniques et la nature de la demande, tout en restant suffisamment souples pour permettre la communication, même s'il manque des informations[43] ; les États poursuivraient les travaux d'élaboration de ces modèles conformément à l'approche par étapes employée pour améliorer le répertoire d'interlocuteurs.

---

[42] Rapport de 2021 du Groupe d'experts gouvernementaux, A/76/135, par. 30 d) ; résolution 76/19 de l'Assemblée générale, adoptée par consensus.

[43] Rapport de 2021 du Groupe d'experts gouvernementaux, A/76/135, par. 77 b) ; résolution 76/19 de l'Assemblée générale, adoptée par consensus.

11. **Partage des informations**. Les informations échangées entre les interlocuteurs doivent rester confidentielles. Les interlocuteurs participant à l'échange d'informations ne doivent partager les informations en question avec des tiers qu'avec le consentement de toutes les parties concernées. Ils sont encouragés à conserver une trace de toutes les informations échangées.

12. **Interaction avec d'autres répertoires**. Le répertoire est une plateforme intergouvernementale et mondiale qui pourrait être complétée par les activités menées aux niveaux régional et sous-régional, le cas échéant. À cet égard, les États ont reconnu que tous les États n'étaient pas membres d'organisations régionales et sous-régionales et que toutes ces organisations ne disposaient pas d'un répertoire d'interlocuteurs. Afin d'éviter les chevauchements d'activités, ils sont encouragés à accorder toute l'attention nécessaire à l'exploitation des synergies avec les répertoires régionaux existants ainsi qu'avec les répertoires existants d'équipes d'intervention informatique d'urgence et d'équipes d'intervention en cas d'atteinte à la sécurité informatique, le cas échéant :

a) Lorsque les États qui établissent la communication sont membres d'une même organisation régionale et que celle-ci est dotée d'un répertoire d'interlocuteurs opérationnel, ils peuvent établir la communication en utilisant soit le répertoire mondial d'interlocuteurs, soit le répertoire d'interlocuteurs de l'organisation régionale concernée. Lorsqu'ils ne sont pas membres de la même organisation régionale, ils peuvent établir la communication en se servant du répertoire mondial ;

b) Si les États ont déjà désigné des interlocuteurs diplomatiques et techniques dans le cadre d'autres répertoires régionaux, ils sont encouragés à désigner les mêmes interlocuteurs diplomatiques et techniques dans le répertoire mondial ;

c) Le cas échéant, le Bureau des affaires de désarmement étudiera, en consultation avec les gestionnaires des répertoires existants, la possibilité de tirer parti des synergies sur le plan technique et la possibilité de mettre régulièrement à jour les informations entre ces répertoires et le répertoire mondial, par l'intermédiaire de canaux de communication adaptés et protégés, lorsque tous les contributeurs au répertoire existant en conviennent.

Renforcement des capacités

13. Guidés par la recommandation figurant dans le premier rapport d'activité annuel invitant les États à « mener des discussions sur les initiatives de renforcement des capacités connexes » en ce qui concerne l'établissement du répertoire d'interlocuteurs, les États conviendront d'un plan d'assistance spécifique, à élaborer conformément aux principes de renforcement des capacités énoncés à l'annexe C, qui comprennent les éléments suivants, à appliquer à titre volontaire, afin d'aider les pays en développement à renforcer les capacités techniques dont ils ont besoin pour participer efficacement au répertoire mondial :

Mesures du Secrétariat de l'ONU

a) Le Secrétariat de l'ONU est invité à mettre au point, en partenariat avec les États intéressés, un tutoriel en ligne « POC 101 » sur les aspects pratiques de la mise en place d'un répertoire d'interlocuteurs et de la participation à un tel mécanisme, afin d'encourager les États à nommer des interlocuteurs nationaux et de faciliter l'utilisation du répertoire par les États ;

b) Le Secrétariat de l'ONU est prié de solliciter les vues des États sur les capacités requises pour participer au répertoire d'interlocuteurs, ce qui pourrait inclure des vues sur les expériences de renforcement des capacités tirées de la participation à d'autres répertoires. Dans ce contexte, il est prié de préparer un

premier document d'information au plus tard en juin 2024 dans lequel il : i) résume les vues présentées par les États ; ii) recense les capacités nécessaires à la participation effective des interlocuteurs au répertoire mondial ; iii) propose des mesures adaptées pour renforcer ces capacités, y compris, entre autres, des programmes sur mesure destinés aux interlocuteurs identifiés ;

c) Le Secrétariat de l'ONU, avec l'appui des États intéressés et des entités pertinentes, est prié d'élaborer une série de modules d'apprentissage en ligne sur mesure portant sur les capacités requises pour que les interlocuteurs participent efficacement au répertoire, telles que recensées dans la note d'information du Secrétariat ;

Mesures du groupe de travail et de sa présidence

d) Au cours des prochaines sessions du groupe de travail, les États mèneront de nouvelles discussions ciblées sur les mesures de suivi qu'il est possible de prendre, en s'appuyant sur les informations présentées dans la note d'information du Secrétariat. Lors de ces discussions, ils feront également le point sur les initiatives compilées sur le site Web du groupe de travail conformément aux alinéas f) et g) du paragraphe 13, et examineront les initiatives supplémentaires qu'il pourrait être nécessaire de mener pour renforcer les capacités recensées dans la note d'information ;

e) Le Président du groupe de travail organisera un exercice de simulation, en partenariat avec les États intéressés, en utilisant des scénarios de base pour permettre aux représentant(e)s des États de simuler les aspects pratiques de la participation à un répertoire d'interlocuteurs et de mieux comprendre les rôles des interlocuteurs diplomatiques et techniques ;

Mesures des États intéressés, à titre volontaire

f) En s'appuyant sur la coopération Sud-Sud, Sud-Nord, triangulaire, sous-régionale et régionale, les États pourraient organiser des réunions d'experts techniques des États qui se préparent à participer au répertoire d'interlocuteurs, en personne ou dans un format hybride, aux niveaux sous-régional, régional, interrégional et mondial, afin de discuter et de partager les expériences relatives à la participation aux répertoires. Ils sont invités à communiquer, dès que possible, ces initiatives au Secrétariat, lequel est prié de les compiler et de les publier au fur et à mesure sur le site Web du groupe de travail ;

g) Les États ou groupes d'États qui en ont la possibilité pourraient appuyer le renforcement des capacités en ce qui concerne le répertoire, y compris en collaboration, selon qu'il convient, avec des organisations régionales et sous-régionales et d'autres parties intéressées, y compris des entreprises, des organisations non gouvernementales et des universités. Ces États sont invités à communiquer, dès que possible, leurs initiatives au Secrétariat, lequel est prié de les compiler et de les publier au fur et à mesure sur le site Web du groupe de travail ; les États sont encouragés à accorder une attention prioritaire aux interlocuteurs désignés pour participer à leurs programmes de renforcement des capacités, le cas échéant.

Poursuite des travaux

14. Le répertoire doit être mis en service le plus rapidement possible. L'amélioration du répertoire se fera de manière progressive et graduelle, conformément aux objectifs et aux principes énoncés ci-dessus. À cet égard, les États pourraient simultanément poursuivre les discussions sur :

a) Les initiatives visant à encourager et à étendre la participation volontaire des États au répertoire ;

b) Les protocoles de communication, y compris le traitement approprié des informations échangées et l'élaboration éventuelle de modèles et de procédures d'interaction ;

c) D'autres idées pour améliorer le fonctionnement du répertoire et sa capacité à faciliter les communications entre les États ;

d) La poursuite des activités de renforcement des capacités visant à permettre la pleine participation des États au répertoire.

15. Le Président du groupe de travail est prié d'organiser régulièrement des réunions des interlocuteurs en présentiel ou en ligne, en commençant par une réunion des interlocuteurs diplomatiques, suivie d'une réunion des interlocuteurs diplomatiques et techniques, afin de partager des informations pratiques et des expériences sur la mise en service et l'utilisation du répertoire.

16. Après la mise en service du répertoire, les États examineront son fonctionnement et étudieront les possibilités de l'améliorer, le cas échéant, y compris par l'échange, entre les États, d'expériences sur l'utilisation du répertoire. À cet égard, il est demandé au Président du groupe de travail de convoquer une réunion en 2024 pour permettre aux États participants d'examiner le fonctionnement et la mise en œuvre du répertoire et d'envisager des améliorations, en tenant compte des objectifs et des principes y relatifs.

Appendice à l'annexe A intitulée « Éléments concernant l'élaboration et la mise en service d'un répertoire mondial et intergouvernemental d'interlocuteurs »

Procédure de demande de renseignements

Les interlocuteurs peuvent suivre les étapes suivantes pour demander des informations à un autre participant concernant un incident touchant la sécurité informatique :

1. Appelez ou envoyez un courriel à l'interlocuteur concerné et indiquez votre nom et votre affiliation.
2. Fournissez autant d'informations que possible sur la nature de l'incident.
3. Demandez des informations complémentaires sur l'incident et précisez vos coordonnées. Si tel est le cas, indiquez que votre demande est urgente.
4. Précisez le canal de communication privilégié et l'agence de votre pays qui deviendra l'interlocuteur principal pour l'incident en question.

Procédure de réponse à une demande de renseignements

Les interlocuteurs peuvent suivre les étapes suivantes pour répondre à une demande de renseignements sur un incident touchant la sécurité informatique :

1. Fournissez une réponse immédiate à la demande de renseignements sur un incident touchant la sécurité informatique (si possible) ; ou
2. Informez l'interlocuteur que vous examinerez l'incident et que vous lui fournirez des renseignements complémentaires. Indiquez le délai de réponse estimé, le cas échéant ; et
3. Convenez du canal de communication privilégié et de l'agence de votre pays qui deviendra l'interlocuteur principal pour l'incident en question.

Annexe B

Liste initiale de mesures de confiance prises volontairement au niveau mondial

La liste suivante est une première liste non exhaustive de mesures de confiance à prendre volontairement au niveau mondial. Ces mesures de confiance sont tirées du rapport final du groupe de travail en 2021 et des premier et deuxième rapports d'activité annuels du groupe de travail. D'autres mesures de confiance pourront être ajoutées à cette liste au fil du temps, le cas échéant, en fonction des discussions menées au sein du groupe de travail.

Mesure de confiance 1
Nommer des interlocuteurs nationaux dans le répertoire mondial d'interlocuteurs, et mettre en service et utiliser le répertoire

a) Les États conviennent d'établir un répertoire mondial et intergouvernemental d'interlocuteurs, en s'appuyant sur les travaux déjà réalisés au niveau régional. Aux quatrième et cinquième sessions du groupe de travail, les États mèneront de nouvelles discussions ciblées sur l'établissement de ce répertoire, sur la base du consensus, ainsi que des discussions sur les initiatives de renforcement des capacités connexes, en tenant compte des meilleures pratiques existantes telles que les expériences régionales et sous-régionales, selon qu'il conviendra.

[Premier rapport d'activité annuel du groupe de travail, section relative aux mesures de confiance, prochaines étapes recommandées, par. 2]

b) Les États qui ne l'ont pas encore fait envisagent de désigner un interlocuteur national, entre autres, aux niveaux technique, politique et diplomatique, en tenant compte des capacités différenciées. Ils sont également encouragés à continuer d'étudier les modalités de l'établissement d'un répertoire d'interlocuteurs au niveau mondial.

[Rapport de 2021 du groupe de travail, par. 51]

c) Les États sont encouragés à mettre en service et à utiliser le répertoire mondial d'interlocuteurs de la manière suivante :

i) Contrôles de communication sous forme de tests « ping » ;

ii) Partage volontaire d'informations, notamment en cas d'incident informatique majeur ou urgent, facilité par le répertoire mondial d'interlocuteurs ;

iii) Exercices de simulation visant à simuler les aspects pratiques de la participation à un répertoire d'interlocuteurs ;

iv) Réunions régulières des interlocuteurs, en ligne ou en présentiel, visant à partager des informations pratiques et des expériences sur la mise en service et l'utilisation du répertoire sur une base volontaire ;

v) Utiliser le répertoire pour établir la communication entre les interlocuteurs, conformément aux modalités du répertoire.

Mesure de confiance 2
Poursuivre les échanges de vues et le dialogue et les consultations bilatérales, sous-régionales, régionales, interrégionales et multilatérales entre les États

a) Les États ont conclu que le dialogue au sein du groupe de travail était en soi une mesure de confiance, car il stimulait un échange de vues ouvert et transparent

sur la perception des menaces et des vulnérabilités, le comportement responsable des États et d'autres acteurs et les bonnes pratiques, ce qui, en fin de compte, encourageait l'élaboration et la mise en œuvre collectives du cadre de comportement responsable des États en matière d'utilisation du numérique.

[Rapport de 2021 du groupe de travail, A/75/816, par. 43]

b) Les États recherchent et étudient les mécanismes permettant un échange interrégional régulier d'enseignements et de bonnes pratiques sur les mesures de confiance, en tenant compte des différences entre les contextes régionaux et quant aux structures des organisations concernées.

[Rapport de 2021 du groupe de travail, A/75/816, par. 52]

c) Les États continuent d'examiner les mesures de confiance aux niveaux bilatéral, régional et multilatéral et promeuvent les mesures qui sont propices à une mise en œuvre coopérative.

[Rapport de 2021 du groupe de travail, par. 53]

d) Les États ont souligné une fois de plus que le groupe de travail lui-même servait de mécanisme de renforcement de la confiance.

[Premier rapport d'activité annuel du groupe de travail, par. 16 e)]

Mesure de confiance 3
Partager, à titre volontaire, des informations telles que les documents de réflexion nationaux, les stratégies, politiques et programmes nationaux, la législation et les meilleures pratiques en matière de TIC

a) Les États, à titre volontaire, continuent à informer le Secrétaire général de leurs vues et observations et à inclure des informations supplémentaires sur les enseignements tirés et sur les bonnes pratiques liées aux mesures de confiance pertinentes prises aux niveaux bilatéral, régional ou multilatéral.

[Rapport de 2021 du groupe de travail, par. 48]

b) Les États s'ouvrent volontairement à des mesures de transparence en partageant les informations et les enseignements pertinents sous le format et dans le cadre des instances de leur choix, selon qu'il convient, y compris via le Portail des politiques de cybersécurité de l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR).

[Rapport de 2021 du groupe de travail, par. 50]

c) Les États sont encouragés à continuer de partager, à titre volontaire, les documents de réflexion, les stratégies, politiques et programmes nationaux, ainsi que les informations sur les institutions et structures liées au numérique présentant un intérêt pour la sécurité internationale, notamment dans le cadre du rapport du Secrétaire général sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, ainsi que dans le Portail des politiques de cybersécurité de l'UNIDIR, selon qu'il convient.

[Premier rapport d'activité annuel du groupe de travail, section relative aux mesures de confiance, prochaines étapes recommandées, par. 5]

Mesure de confiance 4
Promouvoir les possibilités de coopération pour l'élaboration et la mise en œuvre des mesures de confiance

a) Les États, à titre volontaire, définissent et prennent en considération les mesures de confiance adaptées à leur situation particulière et coopèrent avec d'autres États aux fins de leur mise en œuvre.

[Rapport de 2021 du groupe de travail, par. 49]

b) Les États continuent d'examiner les mesures de confiance aux niveaux bilatéral, régional et multilatéral et promeuvent les mesures qui sont propices à une mise en œuvre coopérative.

[Rapport de 2021 du groupe de travail, par. 53]

c) Les États poursuivent, au sein du groupe de travail, les échanges de vues sur l'élaboration et la mise en œuvre des mesures de confiance, notamment sur la possibilité de définir des mesures de confiance supplémentaires.

[Premier rapport d'activité annuel du groupe de travail, section relative aux mesures de confiance, prochaines étapes recommandées, par. 1]

Annexe C

Principes convenus en matière de renforcement des capacités[1]

Prenant en considération et élaborant plus avant des principes largement reconnus, les États ont conclu que le renforcement des capacités liées à l'utilisation des technologies numériques par les États dans le contexte de la sécurité internationale devrait être guidé par les principes suivants :

Processus et finalité

- Le renforcement des capacités doit être un processus durable, prévoyant l'exécution d'activités spécifiques par et pour différents acteurs.
- Ces activités spécifiques doivent avoir une finalité claire et être axées sur les résultats, tout en tendant vers l'objectif commun d'un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies numériques.
- Les activités de renforcement des capacités doivent reposer sur des données factuelles, être politiquement neutres, transparentes, responsables et ne faire l'objet d'aucune condition.
- Le renforcement des capacités doit être entrepris dans le plein respect du principe de la souveraineté des États.
- Il peut être nécessaire de faciliter l'accès aux technologies pertinentes.

Partenariats

- Le renforcement des capacités doit être fondé sur la confiance mutuelle, être axé sur la demande, correspondre aux besoins et priorités recensés au niveau national et être entrepris en tenant pleinement compte de l'appropriation nationale. Les partenaires du renforcement des capacités participent à titre volontaire.
- Les activités de renforcement des capacités devant être adaptées à des besoins et à des contextes spécifiques, toutes les parties sont des partenaires actifs aux responsabilités partagées mais différenciées, s'agissant notamment de collaborer à la conception, à l'exécution, au suivi et à l'évaluation des activités en question.
- La confidentialité des politiques et des plans nationaux doit être protégée et respectée par tous les partenaires.

Personnes

- Le renforcement des capacités doit être respectueux des droits humains et des libertés fondamentales, tenir compte des questions de genre et être inclusif, universel et non discriminatoire.
- La confidentialité des informations sensibles doit être garantie.

[1] Comme convenu dans le rapport final de 2021 du groupe de travail, A/75/816, par. 56.

Annexe D

Liste des documents de travail dans lesquels sont exposées les positions, idées et initiatives des pays et des groupes

(Classés par ordre de date de dépôt, le plus récent en premier, à partir du 27 juillet 2023)

Document de travail sur le portail mondial de coopération en matière de cybersécurité, présenté par l'Inde (texte Rev.1) [version en suivi des modifications]
Inde

Document de travail sur le portail mondial de coopération en matière de cybersécurité, présenté par l'Inde (texte Rev.1) [version corrigée]
Inde

Applicabilité du droit international, en particulier de la Charte des Nations Unies, dans le cadre de l'utilisation du numérique : domaines de convergence, document présenté par un groupe d'États
Plusieurs États (Australie, Colombie, El Salvador, Estonie et Uruguay)

Projet de document de travail actualisé sur la création d'un registre des menaces au sein du système des Nations Unies, présenté par le Kenya
Kenya

Document de position sur l'application du droit international dans le cyberespace, présenté par le Costa Rica
Costa Rica

Document de position sur l'application du droit international dans le cyberespace, présenté par l'Irlande
Irlande

Concept actualisé de la Convention des Nations Unies sur la sécurité internationale de l'information, présenté par la Fédération de Russie (coauteurs : Bélarus, Nicaragua, Syrie, République populaire démocratique de Corée et Venezuela)
Fédération de Russie

Document de travail sur l'applicabilité du droit international, en particulier de la Charte des Nations Unies, dans le cadre de l'utilisation du numérique : domaines de convergence, présenté par un groupe d'États
Plusieurs États (Australie, Colombie, El Salvador et Estonie)

Communication présentée par la France dans le cadre du rapport du Secrétaire général demandé au titre de la résolution 77/37 de l'Assemblée générale
France

Document de travail sur la mise en service provisoire du répertoire d'interlocuteurs, présenté par l'Iran (République islamique d')
Iran (République islamique d')

Document de travail actualisé sur la création d'un registre des menaces au sein du système des Nations Unies, présenté par le Kenya
Kenya

Utilisation du répertoire d'interlocuteurs des Nations Unies pour les questions numériques : communications, partage d'informations et exercices, document présenté par l'Allemagne au nom d'un groupe d'États
Plusieurs États (Allemagne, Argentine, Australie, Brésil, Canada, Chili, Fidji, Israël, Kenya, Mexique, Pays-Bas, République de Corée, République tchèque, Singapour et Uruguay)

Vues sur le futur dialogue institutionnel régulier sur les TIC dans le contexte de la sécurité internationale, document présenté par le Brésil
Brésil

Mesure de confiance n° 1 sur l'établissement d'un répertoire mondial et intergouvernemental d'interlocuteurs, proposition de répertoire de la Fédération de Russie (coauteurs : Bélarus et Nicaragua)
Fédération de Russie

Document de réflexion sur l'établissement, sous l'égide de l'ONU, d'un dialogue institutionnel régulier pour tous les États Membres de l'ONU sur la sécurité et l'utilisation du numérique (coauteurs : Bélarus et Nicaragua)
Fédération de Russie

Document de travail sur le portail mondial de coopération en matière de cybersécurité, présenté par l'Inde
Inde

Document de travail sur la portée, la structure et le contenu du programme d'action proposé pour promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, présenté par l'Égypte
Égypte

Document de position sur l'application du droit international dans le cyberespace, présenté par le Pakistan
Pakistan

Document de réflexion sur le répertoire mondial d'interlocuteurs, présenté par le Venezuela
Venezuela (République bolivarienne du)

Position sur l'établissement d'un répertoire mondial d'interlocuteurs, document présenté par la Jordanie
Jordanie

Vue sur l'établissement d'un répertoire mondial d'interlocuteurs, document présenté par l'Espagne
Espagne

Vues sur le répertoire d'interlocuteurs, document présenté par le Mexique
Mexique

Vues sur un répertoire mondial d'interlocuteurs, document présenté par l'Estonie conformément au premier rapport d'activité annuel (A/77/275)
Estonie

Vue sur l'établissement d'un répertoire mondial d'interlocuteurs, document présenté par la Slovaquie
Slovaquie

Vues préliminaires sur un répertoire mondial d'interlocuteurs, document présenté par la Hongrie
Hongrie

Contributions au répertoire mondial d'interlocuteurs, document présenté par le Maroc conformément au document A/77/275
Maroc

Vue sur le répertoire mondial d'interlocuteurs, document présenté par la République de Corée
République de Corée

Vues nationales sur un répertoire mondial d'interlocuteurs, document présenté par l'Arménie
Arménie

Contributions du Mexique au répertoire mondial d'interlocuteurs
Mexique

Contribution du Sénégal à la note d'information sur un répertoire mondial d'interlocuteurs
Sénégal

Vues sur le répertoire d'interlocuteurs de l'ONU, document présenté par Singapour
Singapour

Vues sur l'établissement d'un répertoire mondial d'interlocuteurs, document présenté par le Pakistan
Pakistan

Vue sur le répertoire mondial d'interlocuteurs, document présenté par la République tchèque conformément au document A/77/275
République tchèque

Position sur le répertoire mondial d'interlocuteurs, document présenté par l'Égypte
Égypte

Vue sur le réseau et le répertoire mondial d'interlocuteurs sur la sécurité numérique, document présenté par l'Italie
Italie

Établissement d'un répertoire d'interlocuteurs, document présenté par l'Inde
Inde

Vue nationale sur le répertoire mondial d'interlocuteurs nationaux, document présenté par El Salvador
El Salvador

Position préliminaire et recommandations sur le répertoire mondial d'interlocuteurs présentées par la Roumanie
Roumanie

Vues sur le répertoire mondial d'interlocuteurs, document présenté par le Royaume-Uni conformément au document A/77/275
Royaume-Uni

Vues sur l'établissement d'un répertoire mondial d'interlocuteurs pour la cybersécurité, document présenté par la France
France

Mise en œuvre de mesures de confiance à l'échelle mondiale dans le domaine numérique : vers le répertoire d'interlocuteurs de l'ONU, document présenté par l'Allemagne au nom d'un groupe d'États
Plusieurs États (Allemagne, Australie, Brésil, Canada, Chili, Fidji, Israël, Mexique, Pays-Bas, République de Corée, Singapour et Uruguay)

Contribution de l'Afrique du Sud à la note d'information sur un répertoire mondial d'interlocuteurs
Afrique du Sud

Vues sur le répertoire mondial d'interlocuteurs, document présenté par la Malaisie
Malaisie

Contribution de la Colombie au répertoire mondial d'interlocuteurs
Colombie

Contribution de l'Allemagne à la note d'information sur un répertoire mondial d'interlocuteurs
Allemagne

Document non officiel sur l'établissement d'un répertoire mondial et intergouvernemental d'interlocuteurs, présenté par la Chine
Chine

Document de réflexion sur l'équivalence fonctionnelle en tant qu'élément essentiel au bon fonctionnement des interlocuteurs, présenté par l'Iran (République islamique d')
Iran (République islamique d')

Document de réflexion sur l'établissement d'un répertoire d'interlocuteurs, présenté par la Fédération de Russie
Fédération de Russie

Document de réflexion actualisé sur une approche pratique du droit international, présenté par le Canada et la Suisse
Plusieurs États (Canada et Suisse)

Note de cadrage présentée par l'Allemagne au nom d'un groupe d'États sur les mesures de confiance
Allemagne

Document de réflexion de la Fédération de Russie sur l'établissement d'un répertoire d'interlocuteurs
Fédération de Russie

Proposition de la Colombie sur le renforcement des capacités
Colombie

Proposition conjointe de l'Allemagne, de l'Australie, du Brésil, du Canada, d'Israël, du Mexique, des Pays-Bas, de la République de Corée et de Singapour sur les mesures de confiance
Plusieurs États (Allemagne, Australie, Brésil, Canada, Israël, Mexique, Pays-Bas, République de Corée et Singapour)

Proposition conjointe de l'Australie, du Botswana, du Chili, du Costa Rica, du Danemark, de l'Indonésie, de la Malaisie, des Pays-Bas et du Royaume-Uni pour le chapitre du rapport d'activité annuel relatif aux menaces (texte Rev.1)
Plusieurs États (Australie, Botswana, Chili, Costa Rica, Danemark, Indonésie, Malaisie, Pays-Bas et Royaume-Uni)

Portail mondial de coopération en matière de cybersécurité : note de cadrage
Inde

Amendements conjoints au rapport d'activité annuel (Bolivie, Cuba, Nicaragua et Venezuela)
Plusieurs États (Bolivie, Cuba, Nicaragua et Venezuela)

Position commune sur le projet de rapport d'activité annuel
Plusieurs États (Fédération de Russie, République arabe syrienne, République bolivarienne du Venezuela, République de Cuba, République du Bélarus, République du Nicaragua et République islamique d'Iran)

Commentaires et propositions de texte des Pays-Bas (sur l'introduction et les menaces existantes et potentielles)
Pays-Bas

Rapport d'activité annuel (texte Rev.1) – Propositions de texte de l'Australie (sur l'introduction, les menaces et les normes)
Australie

Document de travail conjoint sur l'établissement d'un réseau d'interlocuteurs de l'ONU dans le domaine numérique, présenté par un groupe d'États
Plusieurs États (Allemagne, Australie, Brésil, Canada, Israël, Mexique, Pays-Bas, République de Corée et Singapour)

Document de position sur l'application du droit international dans le cyberespace, présenté par la Suède
Suède

Modèle de maturité des capacités en matière de cybersécurité : évaluation des besoins et stratégies nationales, document présenté par plusieurs États
Plusieurs États (Allemagne, Australie, Botswana, Belize, Chili, Colombie, Équateur, Fidji, Géorgie, Islande, Japon, Malawi, Maurice, Pays-Bas, Norvège, Ouganda, Paraguay, Pérou, République dominicaine, Royaume-Uni, Rwanda, Suisse, Tanzanie et Vanuatu)

Promouvoir un programme d'action mondial sur le cyberespace : options et priorités, document présenté par le Canada
Canada

Une approche pratique du droit international au sein du groupe de travail à composition non limitée (2021-2025), document présenté par le Canada et la Suisse
Plusieurs États (Canada et Suisse)

Document de travail visant à faire avancer les discussions menées au sein du groupe de travail des Nations Unies sur les mesures de confiance dans le cyberespace
Plusieurs États

Programme d'exercices de simulation de l'ONU pour les interlocuteurs nationaux pour le cyberespace, présenté par Singapour
Singapour

Note de cadrage sur la bourse consacrée à la cybersécurité établie par l'ONU et Singapour, présentée par Singapour
Singapour

Le droit international applicable au cyberespace, document présenté par le Canada
Canada

Amendements russes au projet de rapport du groupe de travail à composition non limitée du 22 juin 2022
Fédération de Russie

Proposition du Canada pour les travaux du groupe de travail à composition non limitée (2021-2025) sur les progrès accomplis dans le domaine de la sécurité numérique
Canada

Positions de la Chine sur l'élaboration de règles internationales dans le cyberespace
Chine

Initiative mondiale sur la sécurité des données, document présenté par la Chine
Chine

Communication présentée par l'Iran (République islamique d') à la première session de fond
Iran (République islamique d')

Le droit international applicable aux opérations menées dans le cyberespace, document présenté par la France
France

Vues de la Chine sur l'application du principe de souveraineté dans le cyberespace
Chine

Positions de l'Estonie – Groupe de travail à composition non limitée de l'ONU (2021-2025) – Progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale
Estonie

Document de travail pour un programme d'action visant à promouvoir un comportement responsable des États en matière d'utilisation du numérique, présenté par un groupe d'États

Plusieurs États (Allemagne, Argentine, Australie, Autriche, Belgique, Bulgarie, Canada, Chili, Colombie, Croatie, Danemark, Égypte, El Salvador, Émirats arabes unis, Équateur, Espagne, Estonie, France, Finlande, Gabon, Géorgie, Grèce, Guatemala, Hongrie, Irlande, Islande, Italie, Japon, Lettonie, Liban, Liechtenstein, Lituanie, Luxembourg, Malte, Maroc, Monaco, Monténégro, Norvège, Pays-Bas, Pologne, Portugal, République de Chypre, République de Corée, République de Macédoine du Nord, République de Moldova, République tchèque, Roumanie, Royaume-Uni, Singapour, Slovaquie, Slovénie, Suède, Suisse, Ukraine)

Document de position de l'Italie sur le droit international et le cyberespace
Italie

Note sur les travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, présentée par la Fédération de Russie
Fédération de Russie

Document sur l'application du droit international dans le cyberespace, présenté par l'Allemagne
Allemagne

Contribution de la Fédération de Russie aux règles, normes et principes régissant le comportement responsable des États dans l'espace informatique
Fédération de Russie