Nations Unies A/AC.290/2021/L.2

Assemblée générale

Distr. limitée
19 janvier 2021
Français
Original : anglais

Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale

Projet de rapport sur le fond de la question (avant-projet)*

A. Introduction

1. *Malgré les transformations radicales que le monde a connues depuis qu'elle a été créée il y a 75 ans, le but et les idéaux intemporels de l'Organisation des Nations Unies conservent leur pertinence fondamentale. Parallèlement à l'engagement de promouvoir le respect des droits humains et des libertés fondamentales, de favoriser le progrès économique et social de tous les peuples et de créer les conditions nécessaires au maintien du respect du droit international, les États ont pris la résolution d'unir leurs forces pour assurer la paix et la sécurité internationales.*

2. *L'évolution des technologies de l'information et des communications (TIC) a des répercussions sur les trois piliers de l'action menées par les Nations Unies : la paix et la sécurité, les droits humains et le développement durable. Les TIC et la connectivité mondiale ont été un catalyseur du progrès humain et du développement, transformant les sociétés et les économies et élargissant les possibilités de coopération pour le bien commun de l'humanité.*

3. *Il n'a jamais été aussi clair qu'il faut impérativement établir et maintenir la confiance et la sécurité dans l'environnement numérique. Les tendances négatives dans le domaine numérique pourraient compromettre la sécurité et la stabilité internationales, exercer des pressions sur la croissance économique et le développement durable et entraver la pleine jouissance des droits humains et des libertés fondamentales. Il s'agit notamment de l'exploitation croissante des TIC à des fins malveillantes.*

4. *La crise sanitaire mondiale actuelle a mis en évidence les avantages fondamentaux des TIC et notre dépendance à leur égard, notamment pour ce qui est des services publics cruciaux, de la communication de messages essentiels de sécurité publique, de l'élaboration de solutions innovantes pour assurer la continuité des activités, de l'accélération de la recherche et de la contribution au maintien de la*

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

cohésion sociale par des moyens virtuels. En cette période d'incertitude, les États, ainsi que le secteur privé, les chercheurs et d'autres acteurs, ont tiré parti de la technologie numérique pour maintenir les individus et les sociétés en contact et en bonne santé. Dans le même temps, la pandémie de COVID-19 a mis en évidence les risques et les conséquences des activités malveillantes visant à exploiter les vulnérabilités à un moment où les sociétés sont soumises à d'énormes pressions. Elle a également fait ressortir la nécessité de combler les fossés numériques, de renforcer la résilience de chaque société et de chaque secteur et de maintenir une approche centrée sur l'être humain.

5. *Comme les TIC peuvent être utilisées à des fins incompatibles avec l'objectif du maintien de la paix, de la stabilité et de la sécurité internationales, l'Assemblée générale a reconnu que la diffusion et l'emploi des technologies et moyens informatiques intéressent la communauté internationale tout entière et qu'une vaste coopération internationale contribuera à une efficacité optimale*[1].

6. *À la lumière de ce qui précède, le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale créé par la résolution 73/27 de l'Assemblée générale a donné l'occasion d'examiner plus avant cette question cruciale. Il a offert une tribune inclusive à tous les États pour participer, exprimer leurs points de vue et étendre la coopération pour ce qui a trait au volet sécurité internationale des TIC. La participation active des Membres de l'Organisation des Nations Unies et la mobilisation de diverses autres parties prenantes démontrent l'intérêt collectif de la communauté internationale et son aspiration générale à un environnement numérique pacifique et sûr pour tous, ainsi que sa détermination à coopérer pour y parvenir.*

7. *La création du Groupe de travail est l'étape la plus récente en matière de coopération internationale en vue de l'instauration d'un environnement numérique ouvert, sûr, stable, accessible et pacifique. À six reprises depuis 2003, des groupes d'experts gouvernementaux ont été chargés d'étudier les menaces qui se posent ou pourraient se poser dans le domaine de la sécurité numérique, et les mesures de coopération qui pourraient être prises pour y faire face*[2]*. Dans leurs trois rapports de consensus (2010, 2013 et 2015)*[3]*, qui sont cumulatifs par nature, ces groupes ont réaffirmé que le droit international, en particulier la Charte des Nations Unies, est applicable et essentiel au maintien de la paix et de la stabilité dans l'environnement numérique. Ils ont également 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. En outre, des mesures spécifiques de confiance de renforcement des capacités et de coopération, ont été recommandées. Dans la résolution 70/237 de l'Assemblée générale, les États Membres ont convenu par consensus de s'inspirer, pour ce qui touche à l'utilisation de l'informatique et des technologies des communications, du rapport de 2015 du Groupe d'experts gouvernementaux, établissant ainsi plus solidement un premier cadre de comportement responsable des États en matière d'utilisation des TIC.*

8. *Sur cette base, le Groupe de travail a cherché à trouver un terrain d'entente et à assurer la compréhension mutuelle entre tous les États Membres de l'Organisation des Nations Unies quant à un sujet d'importance mondiale. Ses discussions ont été guidées par les principes d'inclusion et de transparence, dans le but de dégager un consensus afin de promouvoir et de maintenir la confiance. Conformément à son mandat, le Groupe de travail a étudié les menaces qui se posent ou pourraient se*

[1] Voir, par exemple, A/RES/53/70, sixième alinéa du préambule.
[2] A/RES/58/32, A/RES/60/45, A/RES/66/24, A/RES/68/243, A/RES/70/237, A/RES/73/266.
[3] A/65/201, A/68/98* et A/70/174.

poser dans le domaine de la sécurité numérique, et les mesures de coopération qui pourraient être prises pour y faire face ; l'élaboration d'autres normes, règles et principes de comportement responsable des États ; la manière dont le droit international s'applique à l'utilisation des TIC par les États ; les mesures de confiance ; le *renforcement des capacités ; et la possibilité d'instaurer un dialogue institutionnel régulier aussi large que possible sous l'égide de l'Organisation des Nations Unies.*

9. *Si les États sont responsables du maintien de la paix et de la sécurité internationales, toutes les parties prenantes ont la responsabilité d'utiliser les TIC d'une manière qui ne mette pas en danger la paix et la sécurité. Comme la dimension sécurité internationale des TIC recoupe de multiples domaines et disciplines, le Groupe de travail a bénéficié de l'expertise, des connaissances et de l'expérience partagées par les représentants des organisations intergouvernementales, des organisations régionales, de la société civile, du secteur privé, des universités et de la communauté technique. La réunion consultative informelle de trois jours qu'il a tenue en décembre 2019 a donné lieu à une riche discussion entre les États et d'autres parties prenantes très diverses*[4]*. Ces parties prenantes ont en outre présenté des propositions concrètes et des exemples de bonnes pratiques dans des contributions écrites et lors d'échanges informels avec le Groupe de travail. Certaines délégations ont également mené de leur propre initiative des consultations multipartites afin d'éclairer leurs contributions au Groupe de travail.*

10. *Ayant à l'esprit que les situations, les capacités et les priorités des États et des régions sont différentes, le Groupe de travail reconnaît que les États ont des responsabilités à la fois individuelles et partagées dans le domaine numérique. Il a conscience que les avantages des technologies numériques ne sont pas répartis de manière égale et que la réduction des fractures numériques, notamment grâce à un accès plus large aux TIC et à la connectivité, reste une priorité urgente pour la communauté internationale.*

11. *Le Groupe de travail se félicite du haut niveau de participation des représentantes déléguées à ses sessions et de la place importante accordée à la dimension de genre dans ses discussions. Il souligne qu'il importe de réduire la « fracture numérique entre les genres » et de promouvoir la participation effective et véritable des femmes aux processus décisionnels liés à l'utilisation des TIC dans le contexte de la sécurité internationale, et leur influence.*

12. *Le Groupe de travail reconnaît l'importance et la complémentarité des discussions d'experts relatives à certains aspects des technologies numériques tenues dans d'autres organes et instances des Nations Unies. Il s'agit notamment des questions liées au développement durable, aux droits humains (y compris la protection des données et de la vie privée, la liberté d'expression et la liberté d'information), à la coopération numérique, à la gouvernance d'Internet, à la cybercriminalité et à l'utilisation d'Internet à des fins terroristes.*

13. *Le Groupe de travail souligne que les différents éléments qui composent son mandat sont interdépendants et se renforcent mutuellement, et qu'ensemble, ils favorisent un environnement numérique ouvert, sûr, stable, accessible et pacifique. Le droit international fournit un cadre pour les mesures prises par les États, et les normes définissent plus précisément les attentes en matière de comportement responsable des États. Les mesures qui accroissent la confiance et les capacités*

[4] Voir le résumé du Président de la réunion consultative informelle intersessions du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale disponible à l'adresse suivante : https://www.un.org/disarmament/open-ended-working-group/.

renforcent l'adhésion au droit international, encouragent la concrétisation de ces normes, offrent des possibilités de coopération accrue entre les États et permettent à chacun d'eux de tirer pleinement parti des avantages des TIC pour sa société et son économie.

14. *Compte tenu de ces synergies, les sections suivantes du rapport sont complémentaires et interdépendantes. Chacune des sections ci-après (B à G) commence par une réflexion sur les points de vue exprimés au cours des discussions de fond du Groupe de travail, suivie d'une énumération des domaines d'accord et de recommandations spécifiques.*

B. Menaces existantes et potentielles

15. Dans leurs discussions au sein du Groupe de travail, les États ont décrit des menaces existantes et potentielles très diverses, mettant en évidence le fait qu'ils peuvent percevoir de différentes manières les menaces liées au domaine numérique. Le format inclusif du Groupe de travail a offert aux États la possibilité d'approfondir leur compréhension de la façon dont les autres perçoivent les actions et les comportements dans l'environnement numérique, et d'entendre ce que les autres considèrent comme les menaces et les risques les plus importants.

Discussions

16. Certains États ont exprimé leur inquiétude quant au développement ou à l'utilisation de capacités numériques à des fins militaires d'une manière incompatible avec les objectifs du maintien de la paix et de la sécurité internationales. Certains ont exprimé la crainte que les caractéristiques de l'environnement numérique n'encouragent des mesures unilatérales plutôt que le règlement des différends par des moyens pacifiques. Des préoccupations ont également été exprimées concernant l'accumulation des vulnérabilités ainsi que le manque de transparence et de processus précis pour les divulguer, l'exploitation des fonctionnalités malveillantes cachées, l'intégrité des chaînes d'approvisionnement mondiales numériques et la garantie de la sécurité des données. Certains États se sont inquiétés de ce que les TIC puissent être utilisées pour s'immiscer dans leurs affaires intérieures, notamment par le biais d'opérations d'information et de campagnes de désinformation. La recherche d'une automatisation et d'une autonomie accrues quant aux opérations informatiques a été présentée comme une préoccupation spécifique, tout comme les mesures qui pourraient conduire à la réduction ou à la perturbation de la connectivité ou à une escalade imprévue, ou avoir des effets préjudiciables sur de tierces parties. Certains États ont également noté le manque de clarté concernant les responsabilités du secteur privé, qui constitue une préoccupation en soi.

17. Les États ont souligné que les mesures visant à promouvoir un comportement responsable des États devaient rester neutres sur le plan technologique, en faisant valoir que c'est l'utilisation abusive des technologies, et non les technologies elles-mêmes, qui est préoccupante. Ils ont reconnu que, même si les progrès technologiques et les nouvelles applications peuvent offrir des possibilités de développement, ils peuvent également étendre les surfaces d'attaque, amplifier les vulnérabilités de l'environnement numérique ou être exploités aux fins d'activités malveillantes nouvelles. Des tendances et des développements technologiques particuliers ont été mis en évidence à cet égard, notamment les progrès de l'apprentissage automatique et de l'informatique quantique ; l'ubiquité des appareils connectés (« Internet des objets ») ; les nouvelles façons de stocker les données et d'y accéder par le biais de

dispositifs d'enregistrement électronique partagés et de l'informatique en nuage ; et l'expansion des mégadonnées et des données personnelles numérisées.

Conclusions

18. Les États ont convenu qu'ils sont de plus en plus préoccupés par les conséquences de l'utilisation malveillante des TIC pour le maintien de la paix et de la sécurité internationales, et par la suite pour les droits humains et le développement. Les incidents informatiques préjudiciables sont de plus en plus fréquents, ciblés et sophistiqués, et ne cessent d'évoluer et de se diversifier. L'augmentation de la connectivité et du recours aux TIC peut entraîner des risques imprévus, rendant les sociétés plus vulnérables aux activités informatiques malveillantes. En dépit des avantages inestimables des technologies de l'information et des communications pour l'humanité, leur utilisation à des fins malveillantes peut avoir des répercussions négatives considérable et de grande envergure.

19. Les États ont convenu que l'augmentation constante du nombre d'incidents impliquant l'utilisation malveillante des technologies de l'information et des communications par des acteurs étatiques et non étatiques, y compris des mandataires, est une tendance inquiétante. Certains acteurs non étatiques ont montré qu'ils disposaient de moyens informatiques qui n'étaient auparavant accessibles qu'aux États, et des inquiétudes ont été exprimées quant au fait que ces capacités pourraient être utilisées à des fins terroristes ou criminelles.

20. Les États ont également convenu que toute utilisation des technologies de l'information et des communications par des États d'une manière incompatible avec l'engagement qu'ils ont pris dans la Charte de vivre en paix l'un avec l'autre dans un esprit de bon voisinage, ainsi qu'avec les autres obligations que leur impose le droit international, mine la confiance et la stabilité entre les États, ce qui peut accroître le risque de perception erronée et la probabilité d'une utilisation dans des conflits futurs entre États.

21. Les États ont convenu que les attaques contre les infrastructures critiques et les infrastructures d'information critiques qui étayent les services essentiels au public, tels que les installations médicales, l'approvisionnement en énergie et en eau, les transports ou l'assainissement, peuvent avoir des conséquences humanitaires désastreuses. Les attaques contre les infrastructures critiques et les infrastructures d'information critiques qui sapent la confiance dans les processus politiques et électoraux et dans les institutions publiques, ou qui ont un impact sur le système financier, sont également une préoccupation réelle et croissante. Ces infrastructures peuvent être détenues, gérées ou exploitées par le secteur privé, partagées ou mises en réseau avec un autre État ou encore exploitées dans différents États. En conséquence, la coopération interétatique ou entre le secteur public et le secteur privé peut être nécessaire pour en protéger l'intégrité, le fonctionnement et l'accès.

22. Les États ont également convenu que l'utilisation des technologies de l'information et des communications aux fins de perturber, endommager ou détruire des infrastructures critiques et des infrastructures d'information critiques constitue une menace non seulement pour la sécurité, mais aussi pour le développement économique et les moyens de subsistance et, en définitive, pour la sécurité et le bien-être des personnes.

23. Les États ont convenu que l'absence de prise de conscience et de moyens adéquats pour détecter les activités malveillantes liées aux TIC, s'en protéger ou y riposter constitue un défi du fait que tous les pays dépendent de plus en plus des

technologies numériques. Comme l'a montré l'actuelle urgence sanitaire mondiale, les vulnérabilités existantes peuvent être amplifiées en temps de crise.

24. Les États ont convenu qu'ils pouvaient vivre différemment les menaces en fonction de leurs niveaux de capacité, de la sécurité et de la résilience de leurs technologies de l'information et des communications, de leur infrastructure et de leur développement. Les menaces peuvent également avoir un impact différent sur différents groupes et entités, notamment sur les jeunes, les personnes âgées, les femmes et les hommes, les populations vulnérables, certaines professions et les petites et moyennes entreprises, entre autres.

25. Compte tenu de la situation de plus en plus préoccupante liée aux menaces numériques, et conscients qu'aucun d'eux n'est à l'abri, les États ont convenu de l'urgence de mettre en œuvre et d'élaborer plus avant des mesures de coopération pour y faire face. Agir ensemble et de manière inclusive chaque fois que cela est possible produirait des résultats plus efficaces et de plus grande portée. L'intérêt de renforcer encore la collaboration, le cas échéant, avec la société civile, le secteur privé, les universités et la communauté technique a également été souligné à cet égard.

C. Droit international

26. Guidés par le mandat du Groupe de travail, en vue de promouvoir une compréhension commune de la manière dont le droit international s'applique à l'utilisation des TIC par les États, les États ont échangé leurs vues sur la manière dont le droit international (principes généraux du droit, traités et droit international coutumier) s'applique à la dimension sécurité internationale des TIC.

Discussions

27. Lors de leurs discussions au sein du Groupe de travail, les États ont rappelé que le droit international et, en particulier, la Charte des Nations Unies, dans son intégralité, sont applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement numérique ouvert, sûr, stable, accessible et pacifique. Ils ont dans le même temps souligné qu'il fallait mieux comprendre comment le droit international s'applique à l'utilisation des TIC par les États.

28. Les principes spécifiques énoncés dans la Charte des Nations Unies et mis en avant dans les discussions sont notamment la souveraineté des États ; l'égalité souveraine ; le règlement des 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 ; le non-recours, dans les relations internationales, 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 ; le respect des droits humains et des libertés fondamentales ; et la non-intervention dans les affaires intérieures d'autres États[5].

29. Il a été rappelé que le droit international est le fondement de la stabilité et de la prévisibilité des relations entre les États. En particulier, le droit international humanitaire réduit les risques et les dommages qui pourraient être causés aux civils et aux biens de caractère civil ainsi qu'aux combattants dans le contexte d'un conflit armé. Dans le même temps, les États ont souligné que le droit international

[5] A/RES/73/27, seizième alinéa du préambule.

humanitaire n'encourage pas la militarisation et ne légitime pas non plus le recours au conflit dans quelque domaine que ce soit.

30. Il a également été noté qu'en vertu du droit international coutumier, la responsabilité des États en ce qui concerne les faits internationalement illicites s'étend à leur utilisation des TIC. Il a été rappelé que les États ne doivent pas faire appel à des intermédiaires pour commettre des faits internationalement illicites à l'aide des technologies numériques et veillent à ce que des acteurs non étatiques agissant sur les instructions ou sous le contrôle d'un État n'utilisent pas leur territoire pour commettre de tels actes. La responsabilité des États a également été relevée en ce qui concerne les entités détenues ou contrôlées par l'État.

31. Les États ont rappelé que le signe qu'une activité numérique a été lancée depuis le territoire ou les infrastructures numériques d'un État ou y trouve son origine peut être insuffisant à lui seul pour imputer l'activité en question à cet État et que les accusations concernant l'organisation et l'exécution d'actes illicites portées contre des États doivent être étayées.

32. Certains États ont estimé que le droit international en vigueur, complété par les normes facultatives et non contraignantes qui reflètent le consensus entre les États, est actuellement suffisant pour traiter la question de l'utilisation des TIC par les États. Il a également été proposé de s'attacher à s'entendre sur la manière dont le cadre normatif déjà convenu s'applique en formulant d'autres orientations, et dont il peut être rendu opérationnel grâce à une meilleure application par tous les États. Dans le même temps, certains États ont estimé qu'en raison de l'évolution rapide du contexte de la menace et de la gravité du risque, un cadre juridiquement contraignant convenu au niveau international est nécessaire. Il a également été suggéré qu'un tel cadre contraignant pourrait conduire à une mise en œuvre plus efficace des engagements au niveau mondial et à l'établissement d'une base plus solide pour tenir les acteurs responsables de leurs actions.

33. Il a été souligné que si les corps existants de règles de droit international ne font pas spécifiquement référence à l'utilisation des TIC dans le contexte de la sécurité internationale, le droit international peut se développer progressivement, notamment par le biais de l'*opinio juris* et de la pratique des États. La possibilité d'élaborer au fil du temps des mesures contraignantes complémentaires parallèlement à la mise en œuvre des normes a été évoquée. Un engagement politique a en outre été proposé pour aller de l'avant.

34. Tout en rappelant que le droit international, et en particulier la Charte des Nations Unies, s'applique à l'utilisation des TIC, des États ont souligné que certaines questions touchant à la manière dont le droit international s'applique à l'utilisation des TIC n'ont pas encore été entièrement clarifiées. Il s'agit notamment du type d'activité liée aux TIC qui pourrait être interprété par d'autres États comme constituant une menace ou un usage de la force (Art. 2, par. 4, de la Charte) ou qui pourrait donner à un État un motif d'invoquer son droit naturel de légitime défense (Art. 51 de la Charte). Il s'agit aussi des questions relatives à la manière dont les principes du droit humanitaire international, tels que les principes d'humanité, de nécessité, de proportionnalité, de distinction et de précaution, s'appliquent aux activités informatiques. À cet égard, certains États ont noté que les discussions sur l'applicabilité du droit international humanitaire à l'utilisation des TIC par les États devaient être abordées avec prudence.

35. Toujours en termes de voies à suivre, les États ont avancé qu'une première étape clé pour clarifier et développer davantage les interprétations communes pourrait résulter d'échanges accrus et de discussions approfondies sur la manière dont s'applique le droit international. Il a été noté que ces échanges pourraient constituer

en eux-mêmes une importante mesure de confiance. Les États ont en outre proposé plusieurs moyens de partager à titre volontaire leurs vues nationales sur la question du droit international, notamment en utilisant le rapport annuel du Secrétaire général sur les progrès de l'informatique et des télécommunications et la sécurité internationale ou en présentant une enquête sur les pratiques nationales en matière d'application du droit international. Les progrès réalisés quant aux accords régionaux et autres accords pour ce qui est d'échanger des points de vue et de parvenir à une compréhension commune de la manière dont le droit international s'applique ont également été soulignés.

36. S'agissant du maintien de la paix et de la prévention des conflits, il a été noté que l'on pourrait également mettre davantage l'accent sur le règlement des différends par des moyens pacifiques et sur le recours à la menace ou à l'emploi de la force. Dans ce contexte, les États ont rappelé les organes, mécanismes et instruments existants pour la prévention et le règlement pacifique des litiges. Certains ont suggéré que la promotion d'une approche et d'une compréhension communes et universellement acceptées de la source des incidents liés aux TIC au niveau technique sous les auspices des Nations Unies, grâce au partage de bonnes pratiques, en gardant à l'esprit le respect du principe de la souveraineté des États, pourrait permettre une meilleure application du principe de responsabilité et une transparence accrue, et contribuer à encourager le recours en justice lorsque des personnes sont lésées par des actes de malveillance.

Conclusions et recommandations

37. En application de la résolution 73/27 de l'Assemblée générale, par laquelle a été créé le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications, les États ont affirmé que le droit international, en particulier la Charte des Nations Unies, était applicable et essentiel au maintien de la paix et de la stabilité et à la création d'un environnement numérique ouvert, sûr, stable, accessible et pacifique. Ils ont également convenu qu'il fallait promouvoir une meilleure compréhension commune de la manière dont le droit international s'applique à l'utilisation des TIC par les États.

38. Les États ont également réaffirmé l'importance du règlement des différends par des moyens pacifiques tels que la négociation, l'enquête, la médiation, la conciliation, l'arbitrage, le règlement judiciaire et le recours aux organismes ou accords régionaux.

39. Les États ont convenu qu'il était possible de favoriser une compréhension commune de la manière dont le droit international s'applique à l'utilisation des TIC par les États en encourageant l'échange de vues sur la question et en identifiant des sujets spécifiques de droit international en vue d'un examen plus approfondi.

40. Afin que tous puissent mieux comprendre la manière dont le droit international s'applique à l'utilisation des technologies numériques par les États, et contribuer à l'établissement d'un consensus au sein de la communauté internationale, les États ont convenu de la nécessité impérieuse de déployer des efforts supplémentaires neutres et objectifs pour renforcer les capacités dans les domaines du droit international, de la législation nationale et de l'élaboration des politiques.

Le Groupe de travail recommande que :

41. Les États, à titre volontaire, continuent de faire part au Secrétaire général de leurs vues et de leurs pratiques nationales quant à la manière dont le droit international s'applique à leur utilisation des technologies numériques dans le contexte de la

sécurité internationale, aux fins de son rapport annuel sur les progrès de l'informatique et des communications dans le contexte de la sécurité internationale.

42. Les États communiquent, à titre volontaire, leurs points de vue et pratiques nationaux sur la manière dont le droit international s'applique à l'utilisation des technologies numériques par les États, au moyen du portail des politiques de cybersécurité (Cyber Policy Portal) de l'Institut des Nations Unies pour la recherche sur le désarmement.

43. Les États qui sont en mesure de le faire continuent de soutenir, de manière neutre et objective, les efforts supplémentaires visant à renforcer les capacités, conformément aux principes énoncés au paragraphe 85 du présent rapport, dans les domaines du droit international, de la législation nationale et de l'élaboration des politiques, afin que tous les États puissent améliorer leur propre compréhension de la manière dont le droit international s'applique à l'utilisation des technologies numériques par les États, et de contribuer à l'instauration d'un consensus au sein de la communauté internationale.

44. Les États continuent d'engager des discussions au niveau multilatéral, afin d'encourager une interprétation commune de la manière dont le droit international s'applique à l'utilisation du numérique par les États dans le contexte de la sécurité internationale, et d'envisager de nouvelles initiatives à cet égard.

D. Normes, règles et principes relatifs au comportement responsable des États

45. Les normes facultatives et non contraignantes de comportement responsable des États jouent 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 reflètent les attentes de la communauté internationale et fixent des critères concernant le comportement des États en matière d'utilisation des technologies de l'information et des communications.

Discussions

46. Dans les discussions au sein du Groupe de travail, il a été rappelé que les normes facultatives et non contraignantes de comportement responsable des États doivent être considérées comme conformes au droit international et aux buts et principes des Nations Unies, notamment le maintien de la paix et de la sécurité internationales et la promotion des droits humains. Les États ont également rappelé la résolution 2131 (XX) de l'Assemblée générale, en date du 21 décembre 1965, intitulée « Déclaration sur l'inadmissibilité de l'intervention dans les affaires intérieures des États et sur la protection de leur indépendance et de leur souveraineté ».

47. Les États ont rappelé que, dans la résolution 70/237, adoptée par consensus, il est demandé aux États de s'inspirer, pour ce qui touche à l'utilisation de l'informatique et des technologies des communications, du rapport de 2015 du Groupe d'experts gouvernementaux, dans lequel sont énoncées 11 normes facultatives et non contraignantes de comportement responsable des États. Certains États ont souligné que ces 11 normes convenues constituaient la base des travaux du Groupe de travail, et d'autres ont également rappelé qu'un ensemble de 13 règles, normes et principes de comportement responsable des États étaient énoncés dans la résolution 73/27 de l'Assemblée générale. Il était de la prérogative des États de mettre progressivement en œuvre des normes facultatives en fonction de leurs priorités et capacités nationales.

48. Les États ont souligné qu'il fallait promouvoir la sensibilisation aux normes existantes et d'en soutenir la mise en œuvre parallèlement à l'élaboration de nouvelles normes au fil du temps. Ils ont fait valoir la nécessité de disposer d'orientations sur la manière de traduire les normes sur le plan opérationnel. À cet égard, ils ont appelé au partage et à la diffusion des bonnes pratiques et des enseignements tirés de la mise en œuvre des normes. Différentes approches concertées ont été proposées, telles qu'une feuille de route élaborée par les États pour les aider dans leurs efforts de mise en œuvre, ainsi que des enquêtes facultatives axées sur la mise en commun des enseignements et des bonnes pratiques.

49. Les États ont constaté que les normes peuvent aider à prévenir les conflits dans le contexte des TIC et contribuer à l'utilisation pacifique et à la pleine réalisation des TIC en vue d'accroître le développement social et économique mondial. Les États ont souligné que l'application des normes ne devrait pas entraîner de restrictions indues en termes de coopération internationale et de transfert de technologie, ni entraver l'innovation à des fins pacifiques et le développement économique des États dans un environnement juste et non discriminatoire. Ils ont également fait valoir les liens entre les normes, le renforcement de la confiance et le renforcement des capacités et ont insisté sur la nécessité d'intégrer la dimension de genre dans la mise en œuvre des normes.

50. Lors des discussions, il a été proposé d'affiner les normes existantes. Les États ont réitéré l'importance de la protection des infrastructures critiques, qui devraient inclure les installations médicales et de soins de santé. Ils ont également attiré l'attention sur le fait qu'il importait de coopérer pour protéger les infrastructures critiques qui transcendent les frontières ou les juridictions, ainsi que l'importance d'assurer la disponibilité générale et l'intégrité d'Internet. Ils ont rappelé la résolution 64/211 de l'Assemblée générale intitulée « Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infostructures essentielles »[6]. Ils ont en outre proposé de mieux assurer l'intégrité de la chaîne d'approvisionnement en produits et services informatiques, en faisant part de leur préoccupation quant aux fonctionnalités cachées malveillantes des produits numériques, et la responsabilité d'aviser les utilisateurs lorsque des vulnérabilités majeures sont identifiées.

51. Dans le prolongement du paragraphe ci-dessus, une liste de propositions écrites formulées par les États dans le cadre des travaux du Groupe de travail au sujet de l'enrichissement des normes existantes, des orientations quant à leur mise en œuvre et de de nouvelles normes ont été compilées dans un document non officiel qui sera mis en ligne[7].

52. Les États ont également pris note du projet de code de conduite international pour la sécurité de l'information présentée en 2015[8].

53. Les États ont reconnu la nécessité d'encourager et de soutenir d'autres initiatives régionales ainsi que des partenariats avec d'autres parties prenantes telles que le secteur privé et la communauté technique pour la mise en œuvre des normes. Ces partenariats pourraient être établis, par exemple, pour garantir des efforts durables de renforcement des capacités afin de remédier aux différences de capacités de mise en œuvre. Les États pourraient être invités à prendre les mesures de sensibilisation et de coopération nécessaires pour que les différentes parties

[6] L'annexe présente un outil d'auto-évaluation volontaire des efforts nationaux visant à protéger les infostructures essentielles.

[7] https://www.un.org/disarmament/open-ended-working-group/.

[8] A/69/723, mentionné dans le document A/70/174, par. 12.

prenantes, y compris les secteurs public et privé et la société civile, assument leurs responsabilités quant à l'utilisation des TIC.

Conclusions et recommandations

54. Les États ont convenu que les normes ne remplacent ni ne modifient les obligations des États en vertu du droit international, qui sont contraignantes, mais fournissent plutôt des orientations spécifiques supplémentaires sur ce qui constitue un comportement responsable de l'État dans l'utilisation des TIC.

55. Les États ont convenu que la pandémie de COVID-19 a accentué l'importance de la protection des infrastructures de soins de santé, y compris les services et les installations médicales, dans le cadre des normes relatives aux infrastructures critiques.

56. Les États ont convenu de l'importance de soutenir et de poursuivre les efforts visant à mettre en œuvre des normes aux niveaux mondial, régional et national.

57. Étant donné la spécificité des TIC, les États ont réaffirmé que, compte tenu des propositions relatives aux normes qui ont été faites dans le cadre du Groupe de travail, de nouvelles normes pourraient continuer à être progressivement élaborées. Ils ont également convenu que l'élaboration de normes et la mise en œuvre de normes existantes ne s'excluaient pas mutuellement mais pouvaient se faire en parallèle.

Le Comité recommande que :

58. Les États, à titre volontaire, passent en revue les efforts faits au niveau national pour mettre en œuvre les normes et continuent à tenir le Secrétaire général informé aux fins de son rapport annuel sur les progrès de l'informatique et des communications dans le contexte de la sécurité internationale. Les États ont par ailleurs demandé au Secrétariat de l'Organisation des Nations Unies de compiler les informations issues de ces enquêtes afin de soutenir les efforts de renforcement des capacités.

59. Les États, en partenariat avec les organisations concernées, notamment l'Organisation des Nations Unies, élaborent de nouvelles orientations facultatives sur la mise en œuvre des normes de comportement responsable des États et les diffusent largement aux niveaux national, régional, interrégional et mondial, et que les États en mesure d'apporter leur expertise et leurs ressources pour contribuer à l'élaboration et à la diffusion de ces orientations soient encouragés à le faire.

60. Les États, en tenant compte des résolutions 70/237 et 73/27 ainsi que, le cas échéant, du document non officiel mentionné au paragraphe 51 contenant les propositions qu'ils ont formulées dans le cadre des travaux du présent Groupe de travail, continuent d'examiner les règles, normes et principes internationaux de comportement responsable des États en matière d'utilisation des TIC dans le contexte de la sécurité internationale, y compris leur mise en œuvre, et d'engager à ce sujet des discussions au niveau multilatéral.

E. Mesures de confiance

61. Les mesures de confiance, qui incluent des mesures de transparence, de coopération et de stabilité, peuvent contribuer à la prévention des conflits ainsi qu'à permettre d'éviter les erreurs d'interprétation et les malentendus, et constituer une « soupape de sécurité » pour la réduction des tensions. Elles sont une expression concrète de la coopération internationale. Accompagnées des ressources, des

capacités et de la volonté nécessaires, les mesures de confiance peuvent renforcer la sécurité, la résilience et l'utilisation pacifique des TIC. Les mesures de confiance peuvent également étayer la mise en œuvre de normes de comportement responsable des États, dans la mesure où elles favorisent la confiance et assurent une plus grande clarté, prévisibilité et stabilité dans l'utilisation des TIC par les États. Avec les autres piliers du cadre de comportement responsable des États, les mesures de confiance peuvent également contribuer à l'instauration d'une communauté de vues entre les États, contribuant ainsi à un environnement international plus pacifique.

62. Comme les mesures de confiance sont des engagements volontaires pris progressivement, elles peuvent constituer une première étape pour dissiper la méfiance entre les États en établissant la communication, en jetant des ponts et en suscitant la coopération autour d'un objectif commun présentant un intérêt mutuel. En tant que telles, les mesures de confiance peuvent poser les bases d'accords et d'arrangements élargis, supplémentaires ou plus structurés dans l'avenir.

Discussions

63. Dans leurs discussions au sein du Groupe de travail, les États ont noté la constante pertinence des mesures de confiance recommandées dans les rapports consensuels de celui-ci. Plusieurs mesures ont été mises en avant comme exigeant une attention prioritaire, telles qu'un dialogue régulier et l'échange à titre volontaire d'informations sur les menaces existantes et émergentes, les grandes orientations ou la doctrine nationales, les points de vue nationaux sur la manière dont le droit international s'applique à l'utilisation des TIC par les États et les stratégies nationales servant à définir les infrastructures critiques et à classer les incidents liés aux TIC. Les échanges de bonnes pratiques dans le cadre des stratégies liées à la criminalistique numérique et aux enquêtes sur les cyberincidents malveillants pourraient à la fois accroître la coopération et renforcer les capacités. L'intérêt de développer une compréhension commune des concepts et de la terminologie a également été souligné comme étant une mesure concrète permettant de faire progresser la coopération internationale et d'instaurer la confiance. Parmi les autres mesures de ce type peuvent être cités l'élaboration d'orientations sur la mise en œuvre des mesures de confiance, la formation des diplomates, l'échange d'enseignements sur la mise en place et l'utilisation de canaux de communication de crise sécurisés, les échanges de personnel, les exercices basés sur des scénarios au niveau de l'élaboration des politiques ainsi que les exercices opérationnels organisés au niveau technique entre les équipes d'intervention rapide dans le domaine informatique ou les équipes d'intervention en cas d'atteinte à la sécurité informatique. Les mesures nationales de transparence, telles que le partage à titre volontaire des réponses à une enquête sur la mise en œuvre de mesures ou la publication de déclarations nationales d'adhésion au cadre de comportement responsable des États, sont d'autres moyens de renforcer la confiance dans les intentions des États et les engagements qu'ils prennent.

64. Compte tenu de l'expérience des organismes régionaux en matière de création et de maintien de réseaux d'interlocuteurs, et en s'appuyant sur les réseaux existants, la viabilité de l'établissement d'un répertoire mondial central d'interlocuteurs a été examinée. Dans le même temps, il a été noté que la sécurité d'un tel répertoire ainsi que ses modalités de fonctionnement seraient cruciales au regard de son efficacité, de même que les efforts pour éviter que les dispositions se chevauchent ou soient excessivement détaillées. L'intérêt de mener régulièrement des exercices au sein d'un réseau d'interlocuteurs a également été souligné, car cela peut contribuer à maintenir l'état de préparation et la réactivité et à garantir que les répertoires d'interlocuteurs soient tenus à jour.

65. Comme les mesures de confiance peuvent être élaborées aux niveaux bilatéral, régional ou multilatéral, les États ont également discuté de l'opportunité et de la viabilité de créer un référentiel mondial des mesures de confiance sous les auspices des Nations Unies, dans le but de mettre en commun les politiques, les bonnes pratiques, les expériences et les évaluations de la mise en œuvre des mesures de confiance et d'encourager l'apprentissage par les pairs et l'investissement en faveur du renforcement des capacités. Un tel référentiel pourrait également aider les États à définir des mesures de confiance supplémentaires correspondant à leur contexte national et régional et offrir des solutions qui pourraient être adaptées ailleurs. Il a été noté qu'un nouveau référentiel mondial, quel qu'il soit, ne devrait pas faire double emploi avec les arrangements existants et que les modalités de son fonctionnement devraient être examinées plus avant.

66. Les États ont également attiré l'attention sur les rôles et responsabilités d'autres acteurs, y compris la société civile, le secteur privé, les universités et la communauté technique, qui contribuent à instaurer la confiance dans l'utilisation des TIC aux niveaux national, régional et mondial. Ils ont souligné la diversité des initiatives multipartites qui, grâce à l'élaboration de principes et d'engagements, ont permis d'établir de nouveaux réseaux d'échange, de collaboration et de coopération. Dans le même ordre d'idées, les initiatives sectorielles ou spécifiques à un domaine ont fait la preuve de la prise de conscience croissante des rôles et responsabilités d'autres acteurs et des contributions uniques qu'ils peuvent apporter à la sécurité des technologies de l'information et des communications par le biais d'engagements pris volontairement, ainsi que de normes et de codes professionnels.

Conclusions et recommandations

67. Les États ont convenu que le dialogue au sein du Groupe de travail était en soi une mesure de confiance, car il stimule 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, encourage l'élaboration et la mise en œuvre collectives du cadre de comportement responsable des États en matière d'utilisation des TIC.

68. En outre, les États ont convenu que l'ONU a un rôle crucial à jouer dans l'élaboration des mesures de confiance mondiales et l'appui à leur mise en œuvre. Des mesures de confiance concrètes ont été recommandées dans chacun des rapports consensuels des groupes d'experts gouvernementaux. Outre ces recommandations spécifiques relatives aux TIC, l'Assemblée générale, dans la résolution consensuelle 43/78 (H), a approuvé les principes directeurs pour l'élaboration de mesures de confiance élaborés dans le cadre de la Commission du désarmement, qui définissent des principes, des objectifs et des caractéristiques utiles pour les mesures de confiance qui peuvent être pris en compte lors de l'élaboration de nouvelles mesures spécifiques aux TIC.

69. S'appuyant sur leurs atouts essentiels que sont la confiance et les relations établies, les États ont reconnu que les organisations régionales et sous-régionales ont déployé des efforts considérables pour élaborer des mesures de confiance, les adapter à leurs besoins et à leurs priorités spécifiques, sensibiliser l'opinion publique et partager l'information entre leurs membres. 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 n'ont pas mis en place des mesures de confiance, il a été noté

que ces mesures sont complémentaires de l'action menée par l'ONU et par d'autres organisations pour promouvoir les mesures de confiance.

70. S'inspirant des leçons et des pratiques partagées au sein du Groupe de travail, les États ont convenu que l'existence préalable de structures et de mécanismes nationaux et régionaux ainsi que la mise en place de ressources et de capacités adéquates, telles que les équipes d'intervention rapide dans le domaine informatique, sont essentielles pour garantir que les mesures de confiance servent l'objectif visé.

71. En tant que mesure spécifique, les États ont convenu que la désignation d'interlocuteurs nationaux est une mesure de confiance en soi, mais qu'elle est également une condition préalable à la mise en œuvre de nombreuses autres mesures de confiance, et qu'elle a une valeur inestimable en temps de crise. Les États peuvent trouver utile d'avoir des interlocuteurs aux fins, entre autres, des échanges diplomatiques, politiques, juridiques et techniques, ainsi que pour le signalement des incidents et les interventions.

Le Groupe de travail recommande que :

72. Les États, à titre volontaire, continuent à informer le Secrétaire général de leurs points de vue et évaluations aux fins de son rapport annuel sur les progrès de l'informatique et des communications dans le contexte de la sécurité internationale, et à inclure des informations supplémentaires sur les enseignements tirés et sur les bonnes pratiques liées aux mesures de confiance pertinentes aux niveaux bilatéral, régional ou multilatéral.

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

74. En tant que mesure de confiance, les États réaffirment publiquement, pour ce qui touche à leur utilisation des TIC, leur engagement à s'inspirer du rapport de 2015 du Groupe d'experts gouvernementaux[9].

75. 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 (Cyber Policy Portal) de l'Institut des Nations Unies pour la recherche sur le désarmement.

76. Les États qui ne l'ont pas encore fait désignent 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 des interlocuteurs au niveau mondial.

77. 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.

78. 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.

[9] A/70/174 ; voir aussi la résolution 70/237.

F. Renforcement des capacités

79. La capacité de la communauté internationale de prévenir ou d'atténuer l'impact d'activités malveillantes dans le domaine des TIC dépend de la capacité de chaque État de se préparer et de réagir. Le renforcement des capacités contribue à mettre en valeur les compétences, les ressources humaines, les politiques et les institutions qui accroissent la résilience et la sécurité des États afin qu'ils puissent bénéficier pleinement des technologies numériques. Le renforcement des capacités est un aspect important de la coopération internationale et constitue un acte volontaire de la part du donateur aussi bien que du bénéficiaire. Il joue un rôle important dans la promotion de l'adhésion au droit international et la mise en œuvre des normes de comportement responsable des États et dans l'appui à la mise en œuvre des mesures de confiance. Dans un monde numériquement interdépendant, les avantages du renforcement des capacités rayonnent au-delà des bénéficiaires initiaux et contribuent à la création d'un environnement numérique plus sûr et plus stable pour tous.

Discussions

80. Dans leurs discussions au sein du Groupe de travail, les États ont souligné la fonction importante que le renforcement des capacités peut jouer en ce qu'il donne à tous les États et aux autres acteurs concernés les moyens de participer pleinement aux discussions menées à l'échelle internationale sur le cadre de comportement responsable des États, tout en contribuant aux engagements communs tels que le Programme de développement durable à l'horizon 2030[10]. À cet égard, les États ont souligné la nécessité d'allouer des ressources financières et humaines suffisantes aux programmes de renforcement des capacités.

81. Les États ont souligné le travail important en matière de renforcement des capacités liées aux TIC qui a été entrepris par d'autres acteurs, notamment les organisations internationales, les organismes régionaux et sous-régionaux, la société civile, le secteur privé, les universités et les organismes techniques spécialisés, et ont encouragé la réflexion sur la manière de promouvoir la coordination, la durabilité, l'efficacité et la réduction des doubles emplois dans ces efforts.

82. L'Organisation des Nations Unies a un rôle essentiel à jouer pour ce qui est d'aider les États à faire mieux connaître le renforcement des capacités et en tirant parti de sa puissance de rassemblement pour promouvoir une meilleure coordination des divers acteurs actifs dans le domaine du renforcement des capacités. Les États ont avancé que les instances existantes au sein du système des Nations Unies, ses institutions spécialisées et la communauté internationale au sens large pourraient être utilisées pour renforcer la coordination déjà établie. Ces instances pourraient être utilisées pour partager les points de vue nationaux sur les besoins en matière de renforcement des capacités, encourager le partage des enseignements tirés et des expériences acquises tant par les bénéficiaires que par les fournisseurs de l'aide et faciliter l'accès aux informations sur les programmes de renforcement des capacités et d'assistance technique. Elles pourraient également promouvoir la mobilisation des ressources ou aider à jumeler les ressources disponibles avec les demandes d'appui au renforcement des capacités et d'assistance technique. Il a été suggéré que

[10] Notamment, mais sans s'y limiter, les objectifs et cibles de développement durable suivants : Accroître nettement l'accès aux technologies de l'information et des communications (9.C) ; Renforcer la coopération Nord-Sud et Sud-Sud et la coopération triangulaire régionale et internationale dans les domaines de la science, de la technologie et de l'innovation et améliorer l'accès à ces domaines (17.6) ; et Apporter, à l'échelon international, un soutien accru pour assurer le renforcement efficace et ciblé des capacités (17.9).

l'élaboration d'un programme mondial de renforcement des capacités cybernétiques sous les auspices des Nations Unies pourrait contribuer à assurer une plus grande cohérence des efforts de renforcement des capacités et que des enquêtes d'auto-évaluation effectuées à titre volontaire pourraient aider les États à identifier et à hiérarchiser leurs besoins en matière de renforcement des capacités ou leur capacité de fournir un appui.

83. Tout en rappelant la responsabilité première des États pour ce qui est de garantir un environnement numérique sûr, sécurisé et fiable, les États ont souligné l'importance d'une approche multipartite du renforcement des capacités qui permette de combler les lacunes techniques et politiques dans tous les secteurs pertinents de la société. Les États ont noté en particulier que la durabilité du renforcement des capacités peut être améliorée grâce à une approche qui implique la collaboration et le partenariat avec la société civile locale, la communauté technique, les institutions universitaires et les acteurs du secteur privé, et grâce à la création de listes d'experts et de pôles de compétences. À cet égard, il a également été souligné que les approches nationales en matière de sécurité numérique pourraient bénéficier de l'adoption d'une approche intersectorielle, globale et multidisciplinaire du renforcement des capacités, notamment en étoffant les organes nationaux de coordination avec la participation des parties prenantes concernées pour évaluer l'efficacité des programmes. Une telle approche peut également aider à relever les défis posés par les technologies naissantes.

84. Les États ont attiré l'attention sur la « fracture numérique entre les genres » et ont demandé instamment que des mesures spécifiques soient prises aux niveaux national et international pour traiter la question de l'égalité des genres et de la participation tangible des femmes aux discussions internationales et aux programmes de renforcement des capacités numériques dans le contexte de la sécurité internationale, notamment en recueillant des données ventilées par genre. Les États ont exprimé leur appréciation pour les programmes qui ont facilité la participation des femmes aux discussions multilatérales sur la sécurité numérique. La nécessité de renforcer les liens entre ce sujet et le programme des Nations Unies pour les femmes et la paix et la sécurité a également été soulignée.

85. Les États ont relevé que de nombreux obstacles entravent ou réduisent l'efficacité du renforcement des capacités. Le manque de coordination et de complémentarité dans l'identification et la mise en œuvre des efforts de renforcement des capacités a été mis en avant comme étant une préoccupation majeure. Les États ont également soulevé des préoccupations d'ordre pratique concernant l'identification des besoins en matière de renforcement des capacités, la rapidité de la réponse aux demandes d'aide au renforcement des capacités, ainsi que la conception, l'exécution, la durabilité et l'accessibilité des activités de renforcement des capacités, et l'absence de mesures spécifiques pour en évaluer l'impact. Dans de nombreux cas, l'insuffisance des ressources humaines, financières et techniques entrave les efforts de renforcement des capacités et les avancées vers la réduction de la fracture numérique. Une fois les capacités renforcées, certains pays doivent relever le défi de la rétention des talents dans un marché concurrentiel pour les professionnels de l'informatique. Les États ont mentionné le fait que le manque d'accès aux technologies liées à la sécurité numérique était également un problème.

Conclusions et recommandations

86. Garantir un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies numériques est une responsabilité commune mais différenciée qui exige une coopération efficace entre les États afin de réduire les risques pour la paix

et la sécurité internationales. Le renforcement des capacités est un élément crucial de cette coopération. Prenant en considération et élaborant plus avant des principes largement reconnus, les États ont convenu 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 identifiés au niveau national et être entrepris en toute reconnaissance 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, sensible à la dimension de genre et inclusif, universel et non discriminatoire.
- La confidentialité des informations sensibles doit être garantie.

87. Les États ont convenu que le renforcement des capacités est une responsabilité partagée en même temps qu'une initiative réciproque, une « voie à double sens », et une occasion pour les participants d'apprendre les uns des autres et pour toutes les parties de bénéficier de l'amélioration générale de la sécurité mondiale en matière de technologies de l'information et des communications. La valeur de la coopération Sud-Sud, Sud-Nord, triangulaire et régionale a également été rappelée.

88. Les États ont convenu que le renforcement des capacités peut contribuer à favoriser la compréhension et la prise en compte des risques systémiques et autres découlant d'une sécurité numérique déficiente, d'une coordination insuffisante entre les capacités techniques et politiques au niveau national et des problèmes connexes que constituent les inégalités et les fractures numériques. Le renforcement des

capacités visant à permettre aux États de recenser et de protéger les infrastructures nationales critiques et d'œuvrer en coopération à la préservation des infrastructures d'information critiques a été jugé particulièrement important. Le partage et la coordination des informations aux niveaux national, régional et international peuvent rendre les activités de renforcement des capacités plus efficaces, plus stratégiques et plus conformes aux priorités nationales.

89. Outre les compétences techniques, le renforcement des institutions et les mécanismes de coopération, les États ont convenu de l'urgence de l'acquisition de compétences spécialisées dans toute une série de domaines à caractère diplomatique, juridique, décisionnel, législatif et réglementaire. Dans ce contexte, l'importance de développer les capacités diplomatiques pour s'engager dans des processus internationaux et intergouvernementaux a été soulignée.

90. Les États ont rappelé la nécessité d'une approche du renforcement des capacités qui soit concrète et orientée vers l'action. Ils ont convenu que des mesures concrètes pourraient inclure un soutien aux niveaux décisionnel et technique, comme l'élaboration de stratégies nationales de cybersécurité, l'octroi d'un accès aux technologies pertinentes, le soutien aux équipes d'intervention rapide dans le domaine informatique ou aux équipes d'intervention en cas d'atteinte à la sécurité informatique et la mise en place de formations spécialisées et de programmes d'études adaptés, y compris des programmes de « formation des formateurs » et de certification professionnelle. Les avantages de la création de centres d'excellence et d'autres mécanismes d'échange d'informations, y compris les bonnes pratiques juridiques et administratives, ont été reconnus.

Le Groupe de travail recommande que :

91. Les États soient guidés par les principes énoncés au paragraphe 86 dans leurs efforts de renforcement des capacités liées aux TIC dans le domaine de la sécurité internationale.

92. Les États, à titre volontaire, continuent de faire part au Secrétaire général de leurs points de vue et évaluations sur les progrès de l'informatique et des communications dans le contexte de la sécurité internationale et d'inclure des informations supplémentaires sur les enseignements tirés et sur les bonnes pratiques liées aux programmes et initiatives de renforcement des capacités.

93. Les États et autres acteurs en mesure d'offrir une aide financière, en nature ou technique en faveur du renforcement des capacités soient encouragés à le faire. Il conviendrait de faciliter davantage la coordination et le financement des efforts de renforcement des capacités, notamment entre les organisations concernées et l'Organisation des Nations Unies.

94. Les États continuent d'envisager de renforcer les capacités au niveau multilatéral, y compris l'échange de vues, d'informations et de bonnes pratiques.

G. Dialogue institutionnel régulier

95. Le Groupe de travail créé par la résolution 73/27 de l'Assemblée générale a offert, pour la première fois sous les auspices des Nations Unies, un espace de dialogue ouvert à tous les États spécialement consacré aux progrès de l'informatique et des communications dans le contexte de la sécurité internationale.

96. Outre la recherche d'un terrain d'entente entre tous les États grâce à des échanges constructifs, comme il ressort des sections précédentes du présent rapport, le Groupe de travail a favorisé les réseaux diplomatiques et encouragé la confiance

entre les participants. La large participation de parties prenantes non gouvernementales a démontré qu'une communauté d'acteurs plus vaste est prête à tirer parti de son expertise pour aider les États à atteindre l'objectif qui est le leur de garantir un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies numériques. Les travaux du Groupe de travail ont confirmé l'importance de discussions récurrentes et structurées sous les auspices des Nations Unies au sujet de l'utilisation des TIC, également reconnue dans les rapports de consensus du Groupes d'experts gouvernementaux.

Discussions

97. Lors de leurs discussions au sein du Groupe de travail, les États ont rappelé le mandat confié à ce dernier dans la résolution 73/27 de l'Assemblée générale, consistant à étudier la possibilité d'instaurer un dialogue institutionnel régulier, et ont confirmé que les évaluations et recommandations du Groupe de travail à cet égard serait un résultat essentiel de ses travaux.

98. Les États ont exprimé diverses opinions quant aux objectifs qui devraient être la priorité d'un futur dialogue institutionnel régulier et quant à la structure de dialogue régulier qui pourrait le mieux concourir à la réalisation de ces objectifs. Certains États ont souhaité un dialogue régulier afin de donner la priorité à la concrétisation des engagements et recommandations existants, notamment l'élaboration d'orientations pour en appuyer et en suivre la mise en œuvre ; la coordination et le renforcement de l'efficacité de la constitution de capacités ; et l'identification et l'échange de bonnes pratiques. D'autres États ont souhaité un dialogue régulier afin de donner la priorité à l'affinage des engagements existants et à la définition de nouveaux engagements, y compris la négociation d'un instrument juridiquement contraignant et des structures institutionnelles qui l'étayent.

99. Certains États ont présenté une proposition spécifique concernant l'établissement d'un programme d'action destiné à favoriser le comportement responsable des États dans le cyberespace en vue d'établir une instance permanente des Nations Unies chargée d'examiner l'utilisation des TIC par les États dans le contexte de la sécurité internationale. Il a été proposé que ce programme d'action constitue un engagement politique des États à respecter les recommandations, normes et principes convenus ; prévoie la tenue régulière de réunions axées sur la mise en œuvre ; intensifie la coopération technique et le renforcement des capacités entre États ; et prévoie l'organisation régulière de conférences d'examen. Une large participation et des consultations étaient également envisagées dans le cadre du projet de programme d'action.

100. Les États ont également souhaité que la communauté internationale revienne à terme à un processus unique ancré dans le consensus et le soutien mondial dès le départ, afin d'assurer la responsabilité collective du processus. À cet égard, ils ont noté que les différents formats proposés pour le dialogue ne s'excluent pas nécessairement les uns les autres. Il a été suggéré que différents formats pourraient être complémentaires ou fusionnés afin de tirer pleinement parti des caractéristiques uniques de chacun et de réduire la duplication des efforts. Il a été proposé que le Groupe de travail élabore une feuille de route dans laquelle seraient définis les thèmes et sujets prioritaires et un calendrier pour le futur dialogue institutionnel régulier.

101. En outre, la nécessité d'examiner plus avant la durée et la pérennité du futur dialogue, la question de savoir s'il doit avoir une vocation délibérative ou être orienté vers l'action, ses échéances, les lieux où il pourrait se tenir et des considérations budgétaires ont également été évoqués.

102. L'examen à l'ONU des progrès de l'informatique et des communications dans le contexte de la sécurité internationale met l'accent sur les aspects liés à la paix et à la stabilité internationales et à la prévention des conflits, et se déroule donc dans le cadre des travaux de la Première Commission de l'Assemblée générale. D'autres organismes des Nations Unies sont mandatés pour examiner les aspects numériques d'autres questions, dont le terrorisme, la criminalité, le développement et les droits humains, ainsi que la gouvernance d'Internet. Il a été suggéré qu'un échange accru entre ces instances et les processus établis par la Première Commission pourrait contribuer à renforcer les synergies et à améliorer la cohérence, tout en respectant les compétences ou le mandat spécialisé de chaque organe.

103. Tout en reconnaissant le rôle et la responsabilité uniques qui sont les leurs en matière de sécurité nationale et internationale, les États ont souligné la contribution importante qu'un comportement responsable des autres acteurs apporte à un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies numériques. Une coopération et des partenariats multipartites accrus peuvent faciliter la création d'un environnement numérique plus résilient et plus sûr.

Conclusions et recommandations

104. Les États ont convenu qu'au vu de la dépendance croissante à l'égard des TIC et l'ampleur des menaces émanant de leur utilisation abusive, il était urgent de renforcer les positions communes, d'instaurer la confiance et d'intensifier la coopération internationale.

105. Les États ont convenu qu'un dialogue suivi favorise la réalisation des objectifs communs que sont le renforcement de la paix et de la stabilité internationale et la prévention des conflits dans l'environnement numérique.

106. Les États ayant la responsabilité première du maintien de la sécurité nationale, de la sûreté publique et de l'état de droit, ils ont convenu de l'importance d'un dialogue intergouvernemental suivi et souligné qu'il fallait définir des mécanismes appropriés pour la collaboration avec d'autres groupes de parties prenantes dans les processus futurs.

107. Les États ont convenu que le dialogue institutionnel régulier établi par la Première Commission devrait rester axé sur la paix et la sécurité internationales afin de ne pas faire double emploi avec les mandats, les initiatives et les activités des Nations Unies axés sur les dimensions numériques d'autres questions, dont le terrorisme, la criminalité, le développement, les droits humains et la gouvernance d'Internet[11].

108. Les États ont convenu que le futur dialogue sur la coopération internationale en matière de TIC dans le contexte de la sécurité internationale devrait, entre autres, sensibiliser l'opinion, instaurer la confiance et encourager des études et des discussions plus approfondies sur les domaines dans lesquels aucune communauté de vues ne s'est encore dégagée.

109. Les États ont convenu qu'un dialogue institutionnel régulier sous les auspices des Nations Unies devrait être un processus orienté vers l'action et assorti d'objectifs spécifiques, qui élargisse la portée des réalisations précédentes et soit inclusif, transparent, fondé sur le consensus et axé sur les résultats.

[11] Voir la note de synthèse publiée par la présidence du Groupe de travail et intitulée « An Initial Overview of UN System Actors, Processes and Activities on ICT-related issues of Interest to the OEWG, By Theme », décembre 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf.

110. Après avoir examiné les aspects de fond de leur mandat, tels qu'ils ressortent des sections B à F du présent rapport, les États ont recommandé, sous chaque section, une liste d'actions concrètes et de mesures de coopération pour faire face aux menaces liées aux TIC et pour promouvoir un environnement numérique ouvert, sûr, stable, accessible et pacifique. Ils ont également convenu de la nécessité de poursuivre le dialogue, notamment en partageant les points de vue nationaux ou les bonnes pratiques sur les questions relatives à l'application du droit international dans le domaine de l'utilisation des TIC ; à la mise en œuvre des normes et à leur évolution dans le temps ; ainsi qu'à l'élaboration et à la mise en œuvre de mesures de renforcement de la confiance et des capacités.

Le Groupe de travail recommande que :

111. Les États tiennent compte des conclusions et recommandations énoncées dans le présent rapport dans tout dialogue institutionnel régulier futur organisé sous les auspices des Nations Unies.

112. Les États établissent un programme pour continuer à donner suite aux accords et engagements existants dans leur utilisation des TIC, comme indiqué dans les résolutions pertinentes de l'Assemblée générale, en particulier la résolution 70/237, ainsi que dans les conclusions et recommandations du présent Groupe de travail. Les discussions se dérouleraient dans le cadre de la Première Commission de l'Assemblée générale des Nations Unies au titre d'un programme d'action destiné à favoriser le comportement responsable des États dans le cyberespace.

113. Les États continuent de participer activement au dialogue institutionnel régulier sous les auspices des Nations Unies.

114. Les États en mesure de le faire envisagent de mettre en place ou d'appuyer des programmes de parrainage et d'autres mécanismes pour assurer une large participation aux processus des Nations Unies susmentionnés.

H. Observations finales

115. Le Groupe de travail a offert à tous les États une occasion historique de s'engager dans des discussions ciblées inscrites dans la durée, sous les auspices des Nations Unies, consacrées à des questions liées aux technologies de l'information et des communications dans le contexte de la sécurité internationale. Outre les nombreux points d'entente dont il est fait état dans le présent rapport, le Groupe de travail a, grâce à ses discussions ouvertes et transparentes, été un moyen précieux d'instaurer la confiance et la compréhension entre les États et a contribué à la mise en place d'un réseau diplomatique mondial d'experts nationaux. La participation vaste et active de toutes les délégations a fait la preuve de la détermination des États à continuer de travailler ensemble sur ce sujet d'une importance fondamentale pour tous.

116. Les réunions formelles, informelles et virtuelles du Groupe de travail ont été caractérisées par des échanges constructifs et interactifs entre les États, ainsi qu'avec la société civile, le secteur privé, les universités et la communauté technique. La détermination dont ont fait preuve les États et les autres parties prenantes tout au long des travaux du Groupe de travail, en multipliant les échanges alors même que certaines de ses réunions sont passées à un format virtuel, est une indication indéniable de la pertinence de plus en plus universelle des sujets qu'il examine ainsi que de la reconnaissance croissante de la nécessité urgente de faire face collectivement aux menaces que l'utilisation des technologies numériques à des fins malveillantes représente pour la sécurité internationale.

117. Le Groupe de travail a montré la volonté collective de la communauté internationale de continuer à collaborer en vue de créer un environnement numérique ouvert, sûr, stable, accessible et pacifique dont bénéficient tous les États et tous les peuples. Tout au long de leurs délibérations au sein du Groupe de travail, les États ont souligné les liens et les synergies entre chacun des éléments de son mandat : les normes volontaires et non contraignantes renforcent et complètent les obligations existantes en vertu du droit international. Ces deux éléments définissent les attentes en matière de comportement concernant les utilisations des TIC par les États dans le contexte de la sécurité internationale. De cette manière, ils contribuent également au renforcement de la confiance en accroissant la transparence et la coopération entre les États et en réduisant le risque de conflit. Le renforcement des capacités permet à son tour à tous les États de contribuer à l'accroissement de la stabilité et de la sécurité à l'échelle mondiale. Ensemble, ces éléments constituent un cadre global de mesures de coopération permettant de faire face aux risques qui se posent ou pourraient se poser dans le domaine des technologies numériques. Un dialogue institutionnel régulier permettra d'élaborer davantage ce cadre et de le rendre opérationnel en faisant progresser une vision commune, en échangeant les enseignements tirés et les bonnes pratiques en matière de mise en œuvre, en renforçant la confiance et en augmentant les capacités des États.