Nations Unies A/76/135

Assemblée générale

Distr. générale
14 juillet 2021
Français
Original : anglais

Soixante-seizième session
Point 96 de la liste préliminaire*
Progrès de l'informatique et des télécommunications et sécurité internationale

Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale

Note du Secrétaire général

Le Secrétaire général a l'honneur de transmettre ci-joint le rapport du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, qui a été créé en application du paragraphe 3 de la résolution 73/266 de l'Assemblée générale.

* A/76/50.

21-04030 (F) 300721 030821

Rapport du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale*

Résumé

Alors que le monde est de plus en plus dépendant des technologies de l'information et des communications, leur utilisation responsable par les États est devenue capitale pour le maintien de la paix et de la sécurité internationales.

Conformément au mandat prévu par la résolution 73/266 de l'Assemblée générale, le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale (2019-2021) a poursuivi l'examen des mesures collectives qui pourraient être prises pour parer aux risques qui se posent ou pourraient se poser dans le domaine de la sécurité informatique, en vue de définir une vision commune et de l'appliquer efficacement.

Le présent rapport contient les conclusions du Groupe dans les domaines suivants : menaces existantes et nouvelles ; normes, règles et principes de comportement responsable des États ; droit international ; mesures de confiance et coopération et assistance internationales en matière de sécurité numérique et de renforcement des capacités. Il permet d'examiner chacune de ces questions en apportant un nouvel éclairage aux conclusions et aux recommandations des précédents groupes d'experts gouvernementaux.

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

Table des matières

Avant-propos du Secrétaire général

Les technologies de l'information et de la communication, qui continuent de transformer rapidement les sociétés, offrent de nombreuses possibilités mais présentent aussi des risques importants. La pandémie de maladie à coronavirus (COVID-19) a encore accéléré la dématérialisation de nombreux aspects de nos vies et notre dépendance à l'égard des technologies numériques.

Dans le même temps, la surveillance et la manipulation numériques sont en plein essor et le monde en ligne évolue d'une manière qui ne sert pas toujours l'intérêt général. Si rien n'est fait, les conséquences pourraient être dévastatrices pour la société et les individus. Il est plus urgent que jamais de relever ces défis, d'exploiter les avantages des technologies de l'information et des communications et de promouvoir un comportement responsable des États dans le contexte de la sécurité internationale.

Afin de s'acquitter de son mandat, le Groupe d'experts gouvernementaux (2019-2021) a mené des réflexions approfondies pendant 18 mois, qui ont été enrichies par des consultations régionales et des réunions informelles ouvertes à tous les États Membres. Le rapport du Groupe et les travaux du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui a adopté un rapport de consensus en mars 2021, sont complémentaires.

Ces dernières années, les États et d'autres acteurs publics et privés ont accordé une importance croissante à l'action menée par l'Organisation des Nations Unies pour promouvoir l'utilisation pacifique des technologies de l'information et des communications. Dans cet esprit, le présent rapport constitue une contribution en faveur d'un environnement numérique ouvert, sûr, stable et accessible. Il s'agit également d'un appel au renforcement de la coopération, afin de réduire les cyberrisques qui menacent la paix et la sécurité internationales et de protéger et promouvoir les droits de l'homme et des libertés fondamentales en ligne et hors ligne.

Lettre d'envoi

28 mai 2021

J'ai l'honneur de transmettre ci-joint le rapport de consensus du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, qui a été créé en 2018 en application du paragraphe 3 de la résolution 73/266 de l'Assemblée générale.

Dans cette résolution, l'Assemblée générale a demandé qu'un groupe d'experts gouvernementaux désignés selon le principe d'une répartition géographique équitable soit créé en 2019, compte tenu des constatations et des recommandations figurant dans les rapports de consensus établis par le Groupe d'experts gouvernementaux en 2010, 2013 et 2015, afin de poursuivre l'examen des mesures collectives qui pourraient être prises pour parer aux risques qui se posent ou pourraient se poser dans le domaine de la sécurité informatique, et notamment des normes, règles et principes de comportement responsable des États, des mesures de confiance et de renforcement des capacités et de la manière dont le droit international s'applique à l'utilisation des technologies de l'information et des communications par les États, en vue de définir une vision commune et de l'appliquer efficacement. Le Secrétaire général a été prié de présenter à l'Assemblée à sa soixante-seizième session un rapport sur les résultats de cette étude.

En application du mandat qui a été confié au Groupe, un recueil officiel des contributions nationales volontaires des experts gouvernementaux sur la question de savoir comment le droit international s'applique à l'utilisation des technologies de l'information et des communications par les États sera publié sur le site Web du Bureau des affaires de désarmement dans la langue de l'original, sans traduction (A/76/136).

Conformément aux termes de la résolution, on a nommé des experts originaires des 25 États suivants : Afrique du Sud, Allemagne, Australie, Brésil, Chine, Estonie, États-Unis d'Amérique, Fédération de Russie, France, Inde, Indonésie, Japon, Jordanie, Kazakhstan, Kenya, Maroc, Maurice, Mexique, Norvège, Pays-Bas, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Singapour, Suisse et Uruguay. On trouvera en annexe au présent rapport la liste des experts.

Le Groupe a tenu quatre sessions officielles : la première du 9 au 13 décembre 2019 au Siège de l'Organisation des Nations Unies, la seconde du 24 au 28 février 2020 à Genève, la troisième de façon virtuelle du 5 au 9 avril 2021 et la quatrième de façon virtuelle du 24 au 28 mai 2021. La troisième session du Groupe a été reportée en raison de la pandémie de COVID-19, en application de la décision 75/551 de l'Assemblée générale. Le Groupe a néanmoins poursuivi ses travaux pendant cette période en organisant une série de consultations intersessions. Conformément à son mandat, il a tenu plusieurs consultations avec les organisations régionales concernées et des réunions consultatives à composition non limitée avec les États Membres, afin que ces derniers puissent prendre part au débat interactif et faire part de leurs vues.

Le Groupe tient à remercier l'équipe d'appui conjointe du Bureau des affaires de désarmement et l'Institut des Nations Unies pour la recherche sur le désarmement de leur contribution.

Je saisis également cette occasion pour remercier personnellement le Gouvernement brésilien de m'avoir désigné et le Groupe de m'avoir fait l'honneur de me confier sa présidence. Je remercie aussi les autres membres du Groupe d'experts, mes collègues brésiliens, les membres de l'équipe d'appui conjointe et le Secrétariat

de l'Organisation des Nations Unies, en particulier la Haute-Représentante pour les affaires de désarmement, de leur soutien et d'avoir partagé leur grande expertise dans un esprit constructif de collaboration.

Le Président du Groupe
(*Signé*) Guilherme **de Aguiar Patriota**

I. Introduction

1. Le présent rapport reflète le résultat des débats tenus par le Groupe d'experts gouvernementaux en application de la résolution 73/266 de l'Assemblée générale intitulée « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale ». Une part importante de ces travaux a été menée pendant la pandémie de maladie à coronavirus (COVID-19), qui a mis en avant le potentiel considérable des technologies numériques tout en accélérant la dépendance du monde à leur égard, ce qui a contribué à souligner davantage l'importance d'adopter un comportement responsable en matière d'utilisation des technologies de l'information et des communications dans le contexte de la sécurité internationale.

2. Le rapport s'appuie sur les évaluations et les recommandations des rapports de consensus établis par les groupes d'experts gouvernementaux des Nations Unies en 2010, 2013 et 2015, qui portaient sur les menaces existantes et nouvelles, les normes, règles et principes volontaires de comportement responsable des États, le droit international, l'instauration d'un climat de confiance, la coopération internationale et le renforcement des capacités ; cet ensemble d'éléments forme un cadre cumulatif et évolutif aux fins du comportement responsable des États dans leur utilisation du numérique. Le Groupe se félicite de l'adoption du rapport de consensus établi par le Groupe de travail à composition non limitée de l'Organisation des Nations Unies sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, créé en application de la résolution 73/27[1] de l'Assemblée générale, qui réaffirme le cadre établi et s'en inspire.

3. Le Groupe d'experts gouvernementaux a examiné les questions relevant de son mandat en tenant compte de leur incidence sur la paix et la sécurité internationales. Il a aussi cherché à apporter un nouveau niveau d'interprétation des recommandations de ses précédents rapports, afin de fournir des orientations permettant de favoriser leur application. Ce niveau supplémentaire réaffirme les liens entre les différents éléments de fond du mandat du Groupe et l'importance de faire participer d'autres acteurs, y compris le secteur privé, la société civile, le monde universitaire et la communauté technique, le cas échéant, aux efforts déployés par les États pour donner suite à ces recommandations.

4. Le Groupe d'experts gouvernementaux reconnaît le rôle important que jouent les organes régionaux et sous-régionaux dans la poursuite des évaluations et des recommandations des rapports des groupes d'experts gouvernementaux de l'Organisation des Nations Unies, ainsi que dans l'élaboration de mécanismes propres aux régions et dans l'intensification des mesures de renforcement des capacités favorisant leur mise en pratique. Conformément au mandat du Groupe, la contribution de ces acteurs et d'autres perspectives et expériences intéressantes ont été partagées lors des réunions consultatives informelles que le Groupe a tenues avec les États Membres à New York et dans le cadre d'une série de consultations organisées en collaboration avec des organisations régionales[2].

5. Le Groupe réaffirme qu'un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies numériques est essentiel pour toutes et tous et nécessite une coopération efficace entre les États afin de réduire les risques pour la paix et la sécurité internationales. Il est dans l'intérêt de tous et vital pour le bien

[1] A/75/816.

[2] Les rapports sur les différentes consultations sont disponibles aux adresses suivantes : https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf et https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf.

commun de promouvoir l'utilisation du numérique à des fins pacifiques. Le respect de la souveraineté, des droits humains et des libertés fondamentales, de même que le développement durable et le développement numérique restent au cœur de ces efforts.

II. Menaces existantes et nouvelles

6. Bien que les technologies de l'information et des communications ainsi que la numérisation et la connectivité croissantes offrent d'immenses possibilités aux sociétés du monde entier, le Groupe réaffirme que les graves menaces liées à ces technologies, mises au jour dans les rapports précédents, persistent. L'utilisation malveillante du numérique par des États et des acteurs non étatiques a gagné en portée, en intensité, en gravité et en sophistication. Ces menaces prennent différentes formes d'une région à l'autre, mais leurs conséquences peuvent être mondiales.

7. Le Groupe d'experts gouvernementaux souligne les évaluations présentées dans le rapport 2015 selon lesquelles plusieurs États mettent au point des technologies numériques à des fins militaires, et la probabilité que ces technologies soient utilisées dans des conflits futurs entre États augmente.

8. Les activités malveillantes menées par les mêmes acteurs, parmi lesquels se trouvent des États et d'autres parties prenantes, peuvent créer un risque important pour la sécurité et la stabilité internationales, pour le développement économique et social ainsi que pour la sécurité et le bien-être des personnes.

9. En outre, les États et d'autres acteurs utilisent activement des capacités numériques plus complexes et sophistiquées à des fins politiques et autres. En outre, le Groupe note avec préoccupation que les États se livrent 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 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.

10. Les activités numériques préjudiciables menées contre des infrastructures critiques fournissant des services à l'échelle nationale, régionale ou mondiale, évoquées dans les rapports précédents, posent une menace de plus en plus sérieuse. Les activités malveillantes liées au numérique qui visent les infrastructures d'information critiques, les infrastructures fournissant des services essentiels au public, les infrastructures techniques essentielles à la disponibilité générale ou à l'intégrité d'Internet et les entités du secteur de la santé sont particulièrement préoccupantes. La pandémie de COVID-19 a mis en évidence les risques et les conséquences des activités malveillantes liées au numérique qui visent à exploiter les vulnérabilités à un moment où les sociétés sont soumises à d'énormes pressions.

11. Les technologies nouvelles élargissent les possibilités de développement. Cependant, leurs propriétés et caractéristiques en constante évolution étendent également les surfaces d'attaques, en créant de nouveaux vecteurs et des vulnérabilités qui peuvent être exploitées aux fins d'activités malveillantes liées au numérique. 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 est devenu un véritable défi.

12. Les capacités de sécurisation des systèmes d'information ne sont pas les mêmes d'un pays à l'autre, tout comme les capacités de développer la résilience, de protéger les infrastructures d'information critiques, de mettre au jour les menaces et d'y répondre rapidement. Ces différences de capacités et de ressources, les disparités qui

existent entre les législations, les règlementations et les pratiques nationales relatives à l'utilisation des technologies numériques, ainsi que le manque d'information sur les mesures de coopération en vigueur aux niveaux régional et mondial qui permettent d'atténuer les effets de telles attaques, d'enquêter sur elles ou de rétablir la situation et l'accès inégal à ces mesures, accroissent les vulnérabilités et les risques auxquels sont exposés tous les États.

13. Le Groupe d'experts gouvernementaux réaffirme que le risque que les technologies de l'information et des communications soient utilisées à des fins terroristes dans le cadre d'autres activités que le recrutement, le financement, l'entraînement et l'incitation au terrorisme, notamment contre des systèmes qui utilisent les technologies du numérique ou contre des infrastructures qui en dépendent, augmente. Si l'on ne s'attaque pas à ce problème, il pourrait menacer la paix et la sécurité internationales.

14. Le Groupe d'experts gouvernementaux réaffirme aussi que la diversité des acteurs non étatiques malveillants, y compris les groupes criminels et les terroristes, leurs motivations différentes, la rapidité avec laquelle les attaques numériques peuvent se produire et la difficulté d'en retrouver la source sont autant de facteurs qui augmentent le risque.

III. Normes, règles et principes de comportement responsable des États

15. En ce qui concerne l'utilisation des technologies numériques par les États, le Groupe d'experts gouvernementaux réaffirme que des normes facultatives et non contraignantes de comportement responsable des États peuvent contribuer à réduire les risques qui pèsent sur la paix, la sécurité et la stabilité internationales. Les normes complètent le droit international en vigueur. Elles ne cherchent pas à limiter ou à interdire des actes qui respectent le droit international. Elles traduisent les attentes de la communauté internationale et fixent des règles de comportement responsable des États. Elles peuvent servir à prévenir les conflits dans l'environnement numérique et contribuer à son utilisation pacifique, afin que ces technologies puissent donner leur pleine mesure en vue d'accroître le développement économique et social à l'échelle mondiale.

16. Le Groupe d'experts gouvernementaux souligne également l'interdépendance entre les normes, les mesures de confiance, la coopération internationale et le renforcement des capacités. Compte tenu des caractéristiques uniques des technologies numériques, il réitère l'observation formulée dans le rapport 2015 selon laquelle des normes supplémentaires pourraient être élaborées au fil du temps et note par ailleurs la possibilité, à l'avenir, de mettre en place des obligations contraignantes, le cas échéant.

17. Outre les travaux menés dans le système des Nations Unies, le Groupe d'experts gouvernementaux se félicite des expériences intéressantes tirées de la mise en œuvre des normes dans les régions, notamment de celles partagées lors des consultations informelles que le Groupe a tenues avec les États Membres à New York et en collaboration avec les organisations régionales, conformément à son mandat, et note que les travaux futurs sur le numérique dans le contexte de la sécurité internationale devraient en tenir compte. Il a aussi pris note du code de conduite international pour la sécurité de l'information proposé par la Chine, la Fédération de Russie, le Kazakhstan, le Kirghizistan, l'Ouzbékistan et le Tadjikistan (voir A/69/723).

18. Dans la résolution de consensus 70/237, l'Assemblée générale a demandé aux États Membres de s'inspirer, pour ce qui touche à l'utilisation du numérique, du

rapport de 2015 du Groupe d'experts gouvernementaux, dans lequel sont énoncées 11 normes facultatives et non contraignantes de comportement responsable des États. En application de son mandat, qui est de promouvoir un comportement responsable, le Groupe d'experts gouvernementaux a élaboré un niveau d'interprétation supplémentaire de ces normes, en soulignant leur valeur pour ce qui est du comportement attendu des États lorsqu'ils utilisent le numérique dans le contexte de la paix et de la sécurité internationales, et en fournissant des exemples de dispositions institutionnelles que les États peuvent prendre à l'échelle nationale et régionale, afin de soutenir leur mise en œuvre. Le Groupe rappelle aux États que ces efforts doivent être menés conformément aux obligations qui leur incombent en vertu de la Charte des Nations Unies et d'autres sources du droit international, en vue de préserver un environnement numérique ouvert, sûr, stable, accessible et pacifique. Les États sont invités à éviter et à s'abstenir d'utiliser les technologies de l'information et des communications de manière non conforme aux normes de comportement responsable des États.

Norme 13 a) : Conformément aux buts de l'Organisation des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, les États devraient coopérer à l'élaboration et à l'application de mesures visant à accroître la stabilité et la sécurité d'utilisation des technologies numériques et à prévenir les pratiques numériques jugées nocives qui peuvent compromettre la paix et la sécurité internationales.

19. Le maintien de la paix et de la sécurité internationales et la coopération internationale font partie des objectifs fondateurs de l'Organisation des Nations Unies. La norme rappelle qu'il s'agit d'une aspiration commune et qu'il est dans l'intérêt de tous les États de coopérer et de collaborer afin de promouvoir l'utilisation du numérique à des fins pacifiques et de prévenir les conflits découlant de leur utilisation malveillante.

20. À cet égard, et en application de cette norme, le Groupe d'experts gouvernementaux encourage les États à s'abstenir d'utiliser les technologies et les réseaux informatiques pour mener des activités qui peuvent menacer le maintien de la paix et de la sécurité internationales.

21. Les mesures recommandées par les précédents groupes d'experts gouvernementaux et le Groupe de travail à composition non limitée constituent un cadre initial pour le comportement responsable des États en matière d'utilisation du numérique. Afin de faciliter la coopération, le Groupe d'experts gouvernementaux recommande également que les États mettent en place des mécanismes, structures et procédures à l'échelle nationale ou renforcent ceux qui existent, notamment les politiques, la législation et les processus d'examen applicables ; les mécanismes de gestion des crises et des attaques ; les accords de coopération et de partenariat à l'échelle de l'ensemble de l'État ; les accords de coopération et de dialogue avec le secteur privé, les universités, la société civile et les milieux techniques. Les États sont aussi encouragés à compiler et à rationaliser les informations qu'ils présentent sur l'application des normes, notamment en menant à titre volontaire des études sur les mesures prises à l'échelon national et en partageant leurs expériences.

Norme 13 b) : En cas d'atteinte à la sécurité numérique, les États devraient examiner toutes les informations utiles, y compris le contexte plus large de l'événement, la difficulté de déterminer les responsabilités dans cet environnement et la nature et l'ampleur des conséquences de l'atteinte.

22. La norme reconnaît que l'attribution de la responsabilité des atteintes numériques est un processus complexe et qu'un large éventail de facteurs doit être pris en compte

avant d'établir la source de ces atteintes. À cet égard, faire preuve de prudence, comme préconisé au paragraphe 71 g) du présent rapport et dans les précédents rapports des groupes d'experts gouvernementaux, peut contribuer à éviter les malentendus et l'escalade des tensions entre les États.

23. Les États qui sont visés par des activités numériques malveillantes et les États sur le territoire desquels de telles activités sont censées avoir été lancées sont invités à consulter les autorités compétentes.

24. Un État victime d'une attaque numérique malveillante devrait prendre en compte tous les aspects dans son évaluation des faits. Ces aspects, étayés par des données factuelles, peuvent inclure les caractéristiques techniques, la portée, l'ampleur et les répercussions de l'attaque, le contexte plus large, notamment son incidence sur la paix et la sécurité internationales et les résultats des consultations entre les États concernés.

25. Lorsqu'il élabore sa réponse à une attaque numérique malveillante imputable à un autre État, l'État touché devrait respecter ses obligations en application de la Charte des Nations Unies et du droit international, notamment celles relatives au règlement pacifique des différends et aux faits internationalement illicites. Les États pourraient également utiliser tous les moyens diplomatiques et juridiques et autres solutions consultatives à leur disposition, ainsi que les mécanismes volontaires et autres dispositifs de collaboration politique qui permettent de régler les désaccords et les différends au moyen de consultations et d'autres voies pacifiques.

26. Pour rendre cette norme opérationnelle à l'échelle nationale, faciliter les enquêtes sur les attaques numériques impliquant d'autres États et régler les problèmes liés à ces attaques, les États peuvent établir ou renforcer les structures, politiques, processus, cadres législatifs et mécanismes de coordination relatifs aux technologies de l'information et des communications applicables à l'échelle nationale, ainsi que les partenariats et les autres formes de dialogue avec les parties prenantes, afin d'évaluer la gravité et la reproductibilité de telles atteintes.

27. La coopération à l'échelle régionale et internationale, notamment entre les équipes d'intervention informatique d'urgence et les équipes d'intervention en cas d'atteinte à la sécurité informatique nationales, les autorités des États chargées du numérique et les milieux de la diplomatie, peut renforcer la capacité des États de détecter des attaques numériques malveillantes et d'enquêter à leur sujet, ainsi que leur capacité d'étayer leurs préoccupations et leurs conclusions avant de se prononcer sur une atteinte.

28. Les États peuvent aussi utiliser les plateformes multilatérales, régionales, bilatérales et multipartites pour mettre en commun des pratiques et des informations sur les démarches adoptées à l'échelle nationale en matière d'attribution, y compris la manière dont ils font la distinction entre les différents types d'attribution, et sur les menaces et atteintes numériques. Le Groupe d'experts gouvernementaux recommande également que l'ONU, dans le cadre de ses futurs travaux, envisage de promouvoir l'adoption d'interprétations communes et l'échange de pratiques en matière d'attribution.

Norme 13 c) : Les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies numériques.

29. La norme reflète l'attente selon laquelle un État, après avoir eu connaissance ou avoir été notifié de bonne foi qu'un fait internationalement illicite utilisant les technologies numériques vient de son territoire ou l'utilise, prendra toutes les mesures adéquates, raisonnablement disponibles et réalistes pour établir les faits, mener une

enquête et résoudre le problème. Elle véhicule l'idée qu'un État ne devrait pas permettre à un autre État ou à un acteur non étatique d'utiliser les technologies numériques sur son territoire pour commettre des faits internationalement illicites.

30. Lorsqu'ils cherchent à savoir comment atteindre les objectifs fixés par cette norme, les États devraient garder à l'esprit les éléments suivants :

a) La norme fait naître l'attente qu'un État prendra des mesures raisonnables, dans les limites de ses moyens, pour mettre fin aux activités en cours sur son territoire, en utilisant des moyens proportionnés, appropriés et efficaces, dans le respect du droit international et du droit interne. Cependant, les États ne sont pas supposés pouvoir ou devoir surveiller toutes les activités numériques menées sur leur territoire ;

b) Un État qui est conscient que, sur son territoire, des faits internationalement illicites sont commis à l'aide des technologies numériques, mais qui n'a pas la capacité d'y faire face, peut envisager de demander l'aide d'autres États ou du secteur privé d'une façon qui respecte le droit international et le droit interne. L'application de cette norme peut être favorisée par la mise en place de structures et de mécanismes permettant de formuler des demandes d'assistance et d'y répondre. Les États doivent agir de bonne foi et conformément au droit international lorsqu'ils fournissent une assistance et ne pas profiter de l'occasion pour mener des activités malveillantes contre l'État demandant assistance ou contre un État tiers ;

c) Un État victime de telles atteintes devrait notifier l'État d'origine. L'État auquel la notification est adressée doit en accuser réception afin de favoriser la coopération et la clarification et prendre toutes les mesures raisonnables pour aider à établir si un fait internationalement illicite a été commis. Le fait d'accuser réception d'une telle notification ne revient pas à approuver les informations qu'elle contient ;

d) Une attaque numérique venant du territoire ou de l'infrastructure d'un État tiers n'implique pas, en soi, que cet État est responsable. 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.

Norme 13 d) : Les États devraient réfléchir à la meilleure façon de coopérer pour échanger des informations, s'assister mutuellement, engager des poursuites en cas d'utilisation terroriste ou criminelle du numérique et appliquer d'autres mesures collectives afin de parer à ces risques. Ils peuvent être amenés à déterminer si de nouvelles mesures doivent être élaborées à cet égard.

31. La norme rappelle aux États que la coopération internationale est importante pour faire face aux menaces transfrontalières créées par l'utilisation du numérique par des terroristes et des criminels, y compris à des fins de recrutement, de financement, de formation et d'incitation, de planification et de coordination d'attaques et de promotion de leurs idées et actions, et à d'autres fins mises en évidence dans le présent rapport. La norme reconnaît que les progrès réalisés dans la réponse à ces menaces et à d'autres menaces de ce type impliquant des individus et des groupes terroristes et criminels peuvent contribuer à la paix et à la sécurité internationales.

32. Le respect de cette norme implique l'existence, à l'échelle nationale, de politiques, de législations, de structures et de mécanismes qui facilitent la coopération transfrontalière sur les questions techniques, répressives, juridiques et diplomatiques relatives à l'utilisation du numérique à des fins criminelles et terroristes.

33. Les États sont encouragés à renforcer et à développer les mécanismes susceptibles de faciliter les échanges d'informations et l'assistance entre les organisations nationales, régionales et internationales compétente, afin de sensibiliser

les États à la sécurité numérique et de réduire les possibilités de mener des actes terroristes et criminels en ligne. Ces mécanismes peuvent renforcer les capacités des organisations et agences concernées tout en instaurant la confiance entre les États et en renforçant le comportement responsable de ceux-ci. Les États sont également encouragés à élaborer les protocoles et les procédures nécessaires à la collecte, au traitement et au stockage des preuves récoltées en ligne concernant l'utilisation du numérique à des fins criminelles et terroristes, et à fournir en temps utile une assistance aux enquêtes, en veillant à ce que ces mesures soient prises conformément aux obligations qui leurs sont faites par le droit international.

34. À l'ONU, un certain nombre d'instances, de processus et de résolutions traitent en particulier des menaces posées par l'utilisation terroriste et criminelle du numérique et des approches coopératives permettant d'y faire face. Parmi les résolutions pertinentes de l'Assemblée générale, citons la résolution 65/230 sur le douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale portant création d'un groupe intergouvernemental d'experts à composition non limitée en vue de faire une étude approfondie du phénomène de la cybercriminalité, la résolution 74/173 visant à favoriser l'assistance technique et le renforcement des capacités pour intensifier l'action nationale et la coopération internationale contre l'utilisation des technologies numériques à des fins criminelles, y compris l'échange d'informations, et la résolution 74/247 sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

35. Les États peuvent aussi utiliser les processus, les initiatives et les instruments juridiques existants et envisager la mise en place d'autres procédures et moyens de communication pour faciliter l'échange d'informations et l'assistance en vue de lutter contre l'utilisation criminelle et terroriste du numérique. À cet égard, les États sont encouragés à continuer de renforcer les efforts actuellement déployés à l'ONU et à l'échelle régionale pour répondre à l'utilisation d'Internet et des technologies de l'information et des communications par les criminels et les terroristes, et à développer à cette fin des partenariats de coopération avec des organisations internationales, les acteurs du secteur, les universités et la société civile.

Norme 13 e) : Les États, lorsqu'ils veillent à une utilisation sûre des technologies numériques, devraient respecter les résolutions 20/8 et 26/13 du Conseil des droits de l'homme sur la promotion, la protection et l'exercice des droits humains sur Internet, ainsi que les résolutions 68/167 et 69/166 de l'Assemblée générale sur le droit à la vie privée à l'ère du numérique afin de garantir le plein respect des droits humains, ainsi que du droit à la liberté d'expression.

36. La norme rappelle aux États de respecter et de protéger les droits humains et les libertés fondamentales, tant en ligne que hors ligne, conformément à leurs obligations respectives. À cet égard, il convient d'accorder une attention particulière au droit à la liberté d'expression, notamment au droit de chercher, de recevoir et de répandre des informations sans considération de frontières et au moyen de tout média, et à d'autres dispositions pertinentes prévues par le Pacte international relatif aux droits civils et politiques, le Pacte international relatif aux droits économiques, sociaux et culturels et la Déclaration universelle des droits de l'homme. Le respect de cette norme peut également contribuer à promouvoir la non-discrimination et à réduire la fracture numérique, y compris entre les genres.

37. L'adoption des résolutions mentionnées dans cette norme, et dans d'autres textes adoptés entre-temps, constitue une reconnaissance du fait que l'utilisation du numérique par les États crée de nouveaux défis et dilemmes, auxquels il faut répondre. Les pratiques des États telles que la surveillance de masse arbitraire ou illégale

peuvent avoir des conséquences particulièrement néfastes sur l'exercice des droits humains, et notamment du droit à la vie privée.

38. Lors de l'application de cette norme, les États devraient tenir compte des orientations contenues dans les résolutions citées. Ils devraient également prendre note des résolutions qui ont été adoptées depuis la publication du rapport du Groupe d'experts gouvernementaux en 2015 et participer à la formulation de nouvelles résolutions dont il pourrait être nécessaire de faire progresser l'élaboration en fonction de l'évolution de la situation.

39. Les mesures prises par les États afin de promouvoir le respect des droits humains et de garantir une utilisation responsable et sûre du numérique devraient être complémentaires, se renforcer mutuellement et être interdépendantes. Une telle démarche favorise un environnement numérique ouvert, sûr, stable, accessible et pacifique, et peut aussi contribuer à la réalisation des objectifs de développement durable.

40. L'innovation technologique est importante pour tous les États, mais les technologies nouvelles peuvent aussi avoir des répercussions notables sur les droits humains et la sécurité informatique. Pour y remédier, les États peuvent envisager d'investir et de faire progresser l'élaboration de mesures techniques et juridiques pour orienter le développement et l'utilisation des technologies, afin que celles-ci soient plus inclusives et accessibles et qu'elles n'aient pas de conséquences néfastes pour les communautés ou les groupes.

41. Le Groupe d'experts gouvernementaux note qu'à l'ONU, un certain nombre d'instances spécialisées sont consacrées aux questions relatives aux droits humains. Il reconnaît aussi que diverses parties prenantes contribuent de différentes manières à la protection et à la promotion des droits humains et des libertés fondamentales, en ligne et hors ligne. Leur participation aux processus d'élaboration des politiques relatives à la sécurité des technologies numériques peut soutenir les activités menées en lien avec la promotion, la protection et l'exercice des droits humains en ligne et contribuer à clarifier et à minimiser les incidences négatives que les politiques pourraient avoir sur les personnes, notamment sur celles qui sont en situation de vulnérabilité.

Norme 13 f) : Un État ne devrait pas mener ou soutenir sciemment une activité numérique qui est contraire aux obligations que lui fait le droit international et qui endommage intentionnellement une infrastructure essentielle ou qui compromet l'utilisation et le fonctionnement d'une infrastructure essentielle à la fourniture de services au public.

42. En ce qui concerne cette norme, une activité numérique qui endommage intentionnellement une infrastructure critique ou qui compromet l'utilisation et le fonctionnement d'une infrastructure essentielle à la fourniture de services au public peut avoir des répercussions en cascade aux niveaux national, régional et mondial. Elle présente un risque élevé de préjudice pour la population et peut entraîner une escalade susceptible de déboucher sur un conflit.

43. Cette norme souligne également le rôle crucial que jouent les infrastructures critiques en qualité de biens nationaux, car ce sont sur elles que reposent les activités et les services essentiels au fonctionnement d'une société. Si ces infrastructures venaient à être gravement compromises ou endommagées, les coûts humains ainsi que les incidences sur l'économie, le développement, la vie politique et sociale d'un pays et sur sa sécurité nationale pourraient être considérables.

44. Aux termes de la norme 13 g), les États devraient prendre les mesures appropriées pour protéger leurs infrastructures essentielles. À ce titre, chaque État

recense les infrastructures ou les secteurs qu'il juge critiques sur le territoire relevant de sa juridiction, en fonction de ses priorités et méthodes de catégorisation.

45. La pandémie de COVID-19 a permis de mieux sensibiliser à l'importance fondamentale de protéger les infrastructures et les installations de soins de santé et de services médicaux, notamment par l'application de normes relatives aux infrastructures essentielles [telles que cette norme et les normes 13 g) et h)]. Parmi les autres exemples de secteurs d'infrastructures critiques qui assurent des services publics essentiels, on peut citer l'énergie et la production d'électricité, l'eau et l'assainissement, l'éducation, les services commerciaux et financiers, les transports, les télécommunications et les processus électoraux. Les infrastructures critiques peuvent également désigner les infrastructures qui fournissent des services dans plusieurs États, comme les infrastructures techniques essentielles à la disponibilité générale ou à l'intégrité d'Internet. De telles infrastructures peuvent jouer un rôle essentiel pour le commerce international, les marchés financiers, les transports dans le monde, les communications, la santé ou l'action humanitaire. Le fait qu'elles soient citées en exemples n'empêche pas les États de qualifier de critiques d'autres infrastructures, pas plus qu'il n'autorise un acte malveillant contre des infrastructures appartenant à des catégories qui ne sont pas susmentionnées.

46. Pour faciliter l'application de cette norme, les États sont encouragés, en complément de la prise en compte des facteurs précités, à adopter les mesures politiques et législatives qui s'imposent au niveau national pour s'assurer que les activités numériques menées ou facilitées par un État qui sont susceptibles d'avoir une incidence sur les infrastructures critiques et la fourniture de services publics essentiels d'un autre État respectent cette norme, que leur utilisation est conforme aux obligations imposées par le droit international, et qu'elles font l'objet d'un examen et d'un contrôle exhaustifs.

Norme 13 g) : Les États devraient prendre les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux technologies numériques en tenant compte de la résolution 58/199 de l'Assemblée générale.

47. Par cette norme, l'ensemble des États réaffirment leur détermination à protéger les infrastructures critiques relevant de leur juridiction des menaces numériques ainsi que l'importance de la coopération internationale dans ce domaine.

48. À cette fin, il peut être utile que les États recensent les infrastructures ou les secteurs qu'ils jugent critiques. Il leur revient également de décider des mesures structurelles, techniques, organisationnelles, législatives et réglementaires à adopter pour protéger leurs infrastructures critiques et rétablir le fonctionnement de celles-ci en cas d'attaque. La résolution 58/199 de l'Assemblée générale, intitulée « Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information », et son annexe[3] décrivent les mesures que les États peuvent prendre à cette fin au niveau national.

49. Certains États hébergent des infrastructures qui assurent des services à l'échelle régionale ou internationale. Les menaces liées aux technologies numériques qui pèsent sur ces infrastructures pourraient avoir des effets déstabilisateurs. Les États concernés pourraient encourager la coopération transfrontière avec les propriétaires et les exploitants concernés afin d'améliorer les mesures de sécurité numérique dont ces infrastructures font l'objet et de renforcer les procédures existantes ou de les compléter en vue de détecter les attaques et d'atténuer leurs effets.

[3] La résolution A/RES/58/199 s'inscrit dans un ensemble de trois résolutions de l'Assemblée générale qui comprend également les résolutions A/RES/57/239 et A/RES/64/211.

50. La facilitation de mesures visant à assurer la sûreté et la sécurité des produits tout au long de leur cycle de vie ou à classer les attaques numériques en fonction de leur ampleur et de leur gravité contribuerait également à la réalisation de l'objectif fixé par cette norme.

Norme 13 h) : Les États devraient répondre aux demandes d'aide appropriées formulées par un autre État dont une infrastructure essentielle est exposée à des actes de malveillance informatique ; ils devraient aussi répondre aux demandes appropriées visant à atténuer les conséquences d'activités numériques malveillantes dirigées contre une infrastructure essentielle d'un autre État et exercées depuis leur territoire, en tenant dûment compte de la souveraineté.

51. La norme rappelle aux États que la coopération internationale, le dialogue et le respect de la souveraineté de tous les États revêtent une importance capitale pour ce qui est de répondre aux demandes d'assistance d'autres États dont les infrastructures critiques sont visées par des activités numériques malveillantes. Elle est particulièrement importante lorsque l'on a affaire à des faits susceptibles de menacer la paix et la sécurité internationales.

52. Lorsqu'ils reçoivent une demande d'assistance, les États devraient offrir leur aide en fonction des capacités et des ressources dont ils disposent et prendre des mesures raisonnables et réalisables à cet égard compte tenu des circonstances. Un État peut choisir de solliciter une assistance à titre bilatéral ou dans le cadre de mécanismes régionaux ou internationaux, ou encore s'adresser au secteur privé pour répondre aux demandes d'assistance reçues.

53. La mise en œuvre effective de cette norme suppose que les structures et les mécanismes nationaux nécessaires aient été mis en place pour détecter et atténuer les attaques numériques susceptibles de menacer la paix et la sécurité internationales. Ces mécanismes viennent compléter les dispositifs existants de gestion courante des attaques numériques et de réponse à celles-ci. Par exemple, il serait utile pour un État souhaitant solliciter l'aide d'un autre État de savoir à qui s'adresser et quel canal de communication utiliser. Un État qui reçoit une demande d'assistance doit évaluer, de la manière la plus rapide et la plus transparente possible et en tenant compte de l'urgence et du caractère sensible de celle-ci, s'il dispose des capacités et des ressources nécessaires pour y donner suite. Les États qui reçoivent une demande d'assistance ne sont pas censés garantir un résultat particulier.

54. La coopération dont il est question dans cette norme peut être facilitée par des processus et des procédures communs et transparents de demande d'assistance à d'autres États et de réponse aux demandes d'assistance. À cet égard, le recours à des modèles communs peut être un moyen de s'assurer que les informations fournies par l'État demandeur sont les plus complètes et précises possible, de manière à faciliter la coopération et à raccourcir les délais de réponse. Ces modèles pourraient être élaborés sur une base volontaire aux niveaux bilatéral, multilatéral ou régional. Le modèle commun de réponse aux demandes d'assistance pourrait, entre autres, permettre d'accuser réception de la demande, et s'il est possible de fournir l'assistance requise, donner des précisions concernant le calendrier, la nature, la portée et les conditions de l'assistance qui pourrait être apportée.

55. Lorsque l'activité malveillante est exercée depuis le territoire d'un État donné, le fait qu'il s'engage à fournir une aide et qu'il s'exécute peut contribuer à limiter les dégâts, à éviter toute méprise, à diminuer les risques d'escalade et à rétablir la confiance. La participation à des mécanismes coopératifs, qui définissent les moyens et le mode de communication à utiliser en cas de crise ainsi que les moyens à mettre

en œuvre pour la gestion et la résolution des incidents, peut renforcer l'application de cette norme.

Norme 13 i) : Les États devraient prendre des mesures raisonnables pour garantir l'intégrité de la chaîne logistique, de sorte que les utilisateurs finaux puissent avoir confiance dans la sécurité des produits numériques, et devraient s'attacher à prévenir la prolifération des techniques et des outils numériques malveillants et l'utilisation de fonctionnalités cachées malveillantes.

56. La norme souligne la nécessité de favoriser la confiance des utilisateurs finaux en un environnement numérique ouvert, sûr, stable, accessible et paisible. À cet égard, et dans l'optique de préserver la sécurité internationale et de favoriser le développement numérique et le développement économique dans son ensemble, il importe de plus en plus de garantir l'intégrité de la chaîne d'approvisionnement du numérique et la sécurité des produits numérique, et de prévenir la prolifération des techniques et des outils numériques malveillants ainsi que l'utilisation de fonctionnalités néfastes et cachées.

57. Très étendues, les chaînes d'approvisionnement mondiales du numérique sont de plus en plus complexes et interdépendantes et elles font intervenir de nombreux acteurs. Parmi les mesures raisonnables permettant de promouvoir l'ouverture et de garantir l'intégrité, la stabilité et la sécurité de ces chaînes, citons :

a) L'instauration au niveau national de cadres et de mécanismes complets, transparents, objectifs et impartiaux de gestion des risques associés à la chaîne d'approvisionnement, qui soient conformes aux obligations internationales des États. Ces cadres pourront englober des estimations des risques tenant compte de divers facteurs, notamment les avantages et les risques des nouvelles technologies ;

b) 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 et des produits et services numériques, d'améliorer la qualité et de promouvoir le choix ;

c) Le renforcement de l'importance accordée, dans les politiques nationales et dans le dialogue avec les États et les acteurs concernés au sein de l'Organisation des Nations Unies et dans les autres enceintes, aux moyens de faire en sorte que tous les États puissent se faire concurrence et innover sur un pied d'égalité, afin que les technologies numériques puissent donner leur pleine mesure en vue d'accroître le développement économique et social à l'échelle mondiale et de contribuer au maintien de la paix et de la sécurité internationales, tout en préservant la sécurité nationale et en défendant l'intérêt général ;

d) 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, aux niveaux bilatéral, régional et multilatéral ; 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 et le recours à d'autres stratégies de réduction des faiblesses de la chaîne d'approvisionnement.

58. Pour prévenir le développement et la prolifération des techniques et des outils numériques malveillants et l'utilisation de fonctionnalités cachées néfastes, telles que les portes dérobées, les États pourront notamment envisager de déployer les solutions suivantes à l'échelle nationale :

a) L'adoption de mesures de renforcement de l'intégrité de la chaîne d'approvisionnement, notamment en demandant aux fournisseurs de produits

numériques de prendre en compte les enjeux de sûreté et de sécurité lors des phases de conception et de développement des produits et tout au long de leur cycle de vie. Cet objectif pourrait également être atteint par la mise en place de procédures de certification indépendantes et impartiales ;

b) Le recours à des mesures législatives et autres, destinées à renforcer la protection des données et de la vie privée ;

c) L'interdiction de l'introduction de fonctionnalités cachées néfastes et de l'exploitation des vulnérabilités des produits numériques, qui sont susceptibles de porter atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes et des réseaux, notamment s'agissant d'infrastructures critiques.

59. En complément des mesures susmentionnées, les États devraient continuer à encourager le secteur privé et la société civile 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, et contribuer ainsi à la réalisation des objectifs fixés par cette norme.

Norme 13 j) : Les États devraient encourager le signalement responsable des vulnérabilités et partager les informations correspondantes sur les moyens permettant de les corriger, afin de limiter et éventuellement d'éliminer les risques pour les systèmes qui utilisent les technologies numériques et pour les infrastructures qui en dépendent.

60. La norme rappelle aux États l'importance 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 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.

61. Les politiques et programmes de divulgation des vulnérabilités numériques, ainsi que la coopération internationale dans ce domaine, ont pour objet l'établissement d'une procédure fiable et cohérente en vue de systématiser ces signalements. Une procédure coordonnée en la matière peut minimiser le préjudice que des produits vulnérables font subir à la société et systématiser le signalement des vulnérabilités ainsi que les demandes d'assistance des pays aux équipes d'intervention d'urgence. Ces procédures doivent être conformes à la législation nationale.

62. Aux niveaux national, régional et international, les États pourraient réfléchir à la mise en place de cadres juridiques, de politiques et de programmes impartiaux visant à orienter la prise de décisions sur le traitement des vulnérabilités numériques et à limiter la distribution commerciale, afin de se prémunir contre toute utilisation abusive faisant peser un risque sur la paix et la sécurité internationales ou sur les droits humains et les libertés fondamentales. Ils pourraient également envisager de prendre des mesures de protection juridique pour les chercheurs et les testeurs d'intrusion.

63. En consultation avec les entreprises du secteur et les autres acteurs de la sécurité numérique concernés, les États peuvent en outre élaborer des orientations et des mesures incitatives compatibles avec les normes techniques internationales applicables dans les domaines suivants : le signalement et la gestion responsables des vulnérabilités ainsi que les rôles et responsabilités respectifs des différentes parties prenantes dans les procédures de signalement ; les types d'informations techniques à divulguer ou à rendre publiques, en particulier en ce qui concerne les atteintes graves

à la sécurité informatique ; le traitement des données sensibles et les moyens de garantir la sécurité et la confidentialité des informations.

64. Les recommandations sur le renforcement de la confiance et la coopération internationale, l'assistance et le renforcement des capacités formulées dans les précédents rapports des Groupes d'experts gouvernementaux peuvent s'avérer particulièrement utiles pour parvenir à une vision commune des mécanismes et processus que les États peuvent instaurer afin de garantir une divulgation responsable des vulnérabilités. À cette fin, les États peuvent envisager de faire appel à des organismes multilatéraux, régionaux et sous-régionaux et à d'autres canaux et plateformes adéquats faisant intervenir différentes parties prenantes.

Norme 13 k) : Les États ne devraient pas mener ou soutenir sciemment des activités visant à porter atteinte aux systèmes d'information des équipes d'intervention d'urgence agréées (parfois également appelées équipes d'intervention informatique d'urgence ou équipes d'intervention en cas d'atteinte à la sécurité informatique) d'un autre État ; un État ne devrait pas se servir d'équipes d'intervention d'urgence agréées pour se livrer à des activités internationales malveillantes.

65. La norme se justifie par le fait que les équipes d'intervention informatique d'urgence, les équipes d'intervention en cas d'atteinte à la sécurité informatique ou les autres équipes autorisées à assurer la gestion et la résolution des incidents informatiques assument des responsabilités et des fonctions clefs, et qu'elles apportent de ce fait une contribution majeure au maintien de la paix et de la sécurité internationales. Elles jouent un rôle capital dans la détection efficace des atteintes à la sécurité informatique et l'atténuation des effets négatifs immédiats et à long terme de celles-ci. Le fait de s'en prendre aux équipes d'intervention d'urgence peut ébranler la confiance et les empêcher d'exercer leurs fonctions, ce qui peut avoir des conséquences plus vastes et souvent imprévisibles pour différents secteurs, voire pour la paix et la sécurité internationales. Le Groupe d'experts gouvernementaux souligne qu'il faut se garder de prêter un caractère politique à ces équipes et respecter le caractère indépendant de leurs fonctions.

66. Compte tenu du rôle essentiel des équipes d'intervention informatique d'urgence et des équipes d'intervention en cas d'atteinte à la sécurité informatique dans la protection de la sécurité nationale et du public et la prévention des pertes économiques découlant d'attaques numériques, de nombreux États estiment qu'elles font partie intégrante de leurs infrastructures critiques.

67. Pour déterminer de quelle manière les mesures qu'ils prennent concernant les équipes d'intervention d'urgence peuvent contribuer à la paix et à la sécurité internationales, les États pourraient déclarer publiquement qu'ils ne se serviront pas d'équipes agréées pour se livrer à des activités malveillantes à l'échelle internationale ou pourraient prendre des dispositions à cet effet, tenir compte des domaines d'activité et des principes éthiques qui orientent le travail de ces équipes et s'y conformer. Le Groupe d'experts gouvernementaux prend note des initiatives récentes en la matière.

68. Les États pourraient également réfléchir à d'autres mesures, comme la mise en place d'un cadre national de gestion des atteintes à la sécurité informatique, qui définirait les rôles et les responsabilités, y compris pour les équipes d'intervention informatique d'urgence et les équipes d'intervention en cas d'atteinte à la sécurité informatique, afin de faciliter la coopération et la coordination entre les équipes et les autres organes techniques et les organismes de sécurité concernés aux niveaux national, régional et international. Ce cadre pourrait comprendre des politiques, des

mesures règlementaires ou des procédures précisant le statut, l'étendue des pouvoirs et les mandats des équipes d'intervention informatique d'urgence et des équipes d'intervention en cas d'atteinte à la sécurité informatique, et établir une distinction entre leurs fonctions propres et celles qui relèvent des gouvernements.

IV. Droit international

69. Fondement de l'engagement commun pris par les États afin de prévenir les conflits et de maintenir la paix et la sécurité internationales, le droit international est essentiel au renforcement de la confiance entre les États. Dans son examen des principes régissant l'application du droit international à l'utilisation du numérique par les États, le Groupe d'experts gouvernementaux réaffirme les évaluations et les recommandations sur le droit international contenues dans les rapports des précédents groupes d'experts gouvernementaux, notamment que le droit international, et en particulier la Charte des Nations Unies, est applicable et essentiel au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement numérique ouvert, sûr, stable, accessible et pacifique. Ces évaluations et recommandations, ainsi que d'autres éléments de fond des rapports précédents, soulignent que le respect par les États du droit international, et en particulier des obligations que leur fait la Charte, constitue un élément essentiel pour leur utilisation du numérique.

70. À cet égard, le Groupe d'experts gouvernementaux a réaffirmé les engagements des États à respecter les principes suivants de la Charte et d'autres principes de droit international : 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 ; la non-intervention dans les affaires intérieures d'autres États.

71. S'appuyant sur les travaux des précédents groupes et guidé par la Charte et par le mandat défini par la résolution 73/266 de l'Assemblée générale, l'actuel Groupe d'experts gouvernementaux propose un nouveau niveau d'interprétation des évaluations et des recommandations présentées dans le rapport de 2015 et exprime les points de vue suivants sur l'applicabilité du droit international à l'utilisation du numérique par les États :

a) Le Groupe d'experts gouvernementaux constate que, en application des obligations qui leur sont faites par l'Article 2 3) et le Chapitre VI de la Charte des Nations Unies, les États parties à tout différend international, y compris en lien avec l'utilisation du numérique, 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 les moyens décrits à l'article 33 de la Charte, à savoir 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. Il note également l'importance d'autres dispositions de la Charte dans le règlement pacifique des différends ;

b) Le Groupe d'experts gouvernementaux réaffirme que la souveraineté étatique et les normes et principes internationaux qui procèdent de la souveraineté s'appliquent à l'utilisation du numérique par les États ainsi qu'à leur compétence territoriale en matière d'infrastructures numériques. Les obligations existantes en application du droit international sont applicables aux activités menées par les États en matière de numérique. Les États peuvent exercer leur compétence sur l'infrastructure numérique se trouvant sur leur territoire, notamment en élaborant des mesures et des

lois et en établissant les mécanismes nécessaires pour protéger ladite infrastructure contre les menaces numériques ;

c) Conformément au principe de non-intervention, les États n'ont pas le droit d'intervenir directement ou indirectement dans les affaires intérieures d'un autre État, notamment au moyen des technologiques numériques ;

d) Lorsqu'ils utilisent les technologies numériques, et en application de la Charte des Nations Unies, les États doivent s'abstenir, 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 ;

e) Soulignant les aspirations de la communauté internationale à l'utilisation pacifique du numérique pour le bien commun de l'humanité et rappelant que la Charte des Nations Unies s'applique dans son intégralité, le Groupe d'experts gouvernementaux a noté que les États avaient implicitement le droit de prendre des mesures conformes au droit international et reconnues par la Charte et qu'il fallait poursuivre les recherches dans ce domaine ;

f) 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 ;

g) Le Groupe d'experts gouvernementaux réaffirme que les États sont tenus de remplir leurs obligations internationales quant aux faits internationalement illicites qui leur sont imputables en droit international. Il réaffirme également que les États ne doivent pas faire appel à des intermédiaires pour commettre des faits internationalement illicites à l'aide des technologies numériques et devraient veiller à ce que des acteurs non étatiques n'utilisent pas leur territoire pour commettre de tels actes. Il rappelle toutefois 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 note que les accusations concernant l'organisation et l'exécution d'actes illicites portées contre des États doivent être étayées. L'invocation de la responsabilité des États pour un fait internationalement illicite comporte des aspects juridiques, techniques et politiques complexes.

72. Sans préjudice du droit international en vigueur et des évolutions futures du droit international, le Groupe d'experts gouvernementaux a reconnu que la poursuite des discussions et des échanges de vues entre les États, collectivement à l'Organisation des Nations Unies, sur la manière dont des règles et principes particuliers du droit international s'appliquent à l'utilisation du numérique par les États est essentielle pour approfondir les interprétations communes, éviter les malentendus et accroître la prévisibilité et la stabilité. Ces discussions pourraient être éclairées et favorisées par des échanges de vues entre les États, au niveau régional ou de façon bilatérale.

73. En application du mandat qui a été confié au Groupe d'experts gouvernementaux, un recueil officiel des contributions nationales volontaires des experts gouvernementaux sur la question de savoir comment le droit international s'applique à l'utilisation des technologies numériques par les États sera publié sur le site Web du Bureau des affaires de désarmement. Le Groupe encourage tous les États à continuer de partager

volontairement leurs points de vue et leurs évaluations nationales par l'intermédiaire du Secrétaire général et par d'autres moyens, le cas échéant.

V. Mesures de confiance

74. Le Groupe d'experts gouvernementaux note que les mesures de confiance, qui permettent d'accroître la confiance, la coopération, la transparence et la prévisibilité, peuvent promouvoir la stabilité et contribuer à réduire le risque de méprise, d'escalade et de conflit. L'instauration de la confiance est une entreprise progressive et de longue haleine, qui suppose un engagement constant des États. Le soutien de l'ONU, des organismes régionaux et sous-régionaux et des autres parties prenantes peut contribuer à la mise en œuvre effective et au renforcement des mesures de confiance.

75. À l'appui de leur action visant à instaurer la confiance et à garantir un environnement numérique pacifique, les États sont encouragés à réaffirmer publiquement leur engagement à l'égard du cadre de comportement responsable mentionné au paragraphe 2, et à s'y conformer. Ils sont également invités à tenir compte des principes directeurs pour l'élaboration de mesures de confiance que la Commission du désarmement de l'ONU a adoptés en 1988 et qui ont été approuvés par consensus par l'Assemblée générale dans sa résolution 43/78 (H), et à étudier les pratiques relatives aux mesures de confiance et à leur mise en œuvre, qui ont récemment fait leur apparition à l'échelle régionale et sous-régionale.

Mesures de coopération

Points de contact

76. Le recensement des points de contact appropriés aux niveaux décisionnel et technique 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 points de contact 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.

77. S'agissant de la désignation de points de contact ou de leur propre participation aux réseaux de points de contact, les États pourraient intégrer à leur réflexion les éléments suivants :

a) La désignation de points de contact dédiés aux niveaux décisionnel, diplomatique et technique et la fourniture d'orientations concernant la définition de leurs attributions, notamment des fonctions qu'ils sont censés exercer, de leur rôle en matière de coordination et des exigences de disponibilité les concernant ;

b) La mise en place de procédures intergouvernementales et intragouvernementales en vue de permettre aux points de contact de communiquer efficacement en cas de crise, notamment grâce au recours à des modèles normalisés précisant les types d'informations à fournir, en particulier les caractéristiques techniques et la nature de la demande, mais qui restent suffisamment souples pour permettre la communication, même s'il manque des informations ;

c) La mise à profit des enseignements et des bonnes pratiques tirés des réseaux régionaux de points de contact, notamment en ce qui concerne la réflexion sur les méthodes pratiques relatives à l'utilisation des réseaux de points de contact

dans des contextes nationaux, régionaux et internationaux, y compris pour la détection précoce des incidents informatiques graves, dans le but de renforcer la coordination et le partage d'informations entre les points de contact désignés, ainsi que l'élaboration et la mise en œuvre de ces méthodes.

78. La lutte contre les menaces qui pèsent sur la sécurité numérique dans le monde passe également par la mise en œuvre d'approches mondiales à la fois inclusives et universelles. Les États pourraient inviter le Secrétaire général de l'ONU à faciliter les échanges volontaires entre tous les États Membres sur les enseignements, les bonnes pratiques et les orientations concernant les réseaux de points de contact déjà en place aux niveaux régional et sous-régional. Ces travaux pourraient alimenter les débats dans l'optique de la création d'un répertoire mondial des points de contact.

Dialogue et consultations

79. Le dialogue mené dans le cadre de consultations et de collaborations bilatérales, sous-régionales, régionales et multilatérales peut améliorer la compréhension entre les États, favoriser un renforcement de la confiance et contribuer à resserrer la coopération interétatique en vue d'atténuer les attaques numériques, tout en limitant les risques de méprise et d'escalade. D'autres parties prenantes, telles que le secteur privé, les universités, la société civile et les milieux techniques, peuvent grandement contribuer à faciliter ces consultations et ces collaborations.

80. Les organismes régionaux ont pris des dispositions notables afin d'élaborer et de mettre en œuvre des mesures de confiance visant à réduire le risque de méprise, d'escalade et de conflit susceptible de découler d'attaques numériques. La participation aux activités de ces organismes régionaux permet de porter l'attention sur les caractéristiques et les préoccupations propres à chaque région, tandis que les échanges interrégionaux favorisent l'apprentissage mutuel entre ces organismes. Les États sont encouragés à poursuivre ce travail et à coopérer activement avec les États qui ne sont pas actuellement membres d'une organisation régionale ou sous-régionale concernée.

81. Pour continuer à renforcer les mesures de coopération intéressant les équipes d'intervention informatique d'urgence nationales et d'autres organes compétents, les États pourraient encourager le partage et la diffusion d'informations et de bonnes pratiques sur la mise en place et le maintien au niveau national d'équipes d'intervention informatique d'urgence et d'équipes d'intervention en cas d'atteinte à la sécurité informatique, ainsi que sur la gestion des attaques numériques dans le cadre des organisations et réseaux régionaux et mondiaux d'intervention d'urgence déjà créés. Les encouragements et l'appui donnés à ces équipes permettraient également de sensibiliser les États aux engagements qu'ils ont pris au titre de la norme 13 k) envers elles et envers d'autres organes apparentés.

Mesures de transparence

82. Pour instaurer un climat de confiance et de prévisibilité, réduire les risques de méprise et de surenchère et aider les institutions et les organismes à prendre de bonnes décisions en matière de gestion des risques, il est important que les pays fassent volontairement preuve de transparence en échangeant leurs points de vue et leurs pratiques sur les atteintes à la sécurité numérique et d'autres menaces et en mettant à la disposition de tous des conseils, des orientations, un corpus de données factuelles et des données facilitant la prise de décisions.

83. Pour continuer d'améliorer la transparence et la prévisibilité du comportement des États, permettre l'accès à un plus large éventail de vues et d'expériences, renforcer le niveau de préparation des États et leur permettre de détecter au plus tôt

les nouvelles menaces, ceux-ci pourraient envisager de mettre à profit les instances bilatérales, sous-régionales, régionales et multilatérales et les consultations informelles pour échanger volontairement : des informations et des bonnes pratiques, des enseignements tirés de leur expérience ou des livres blancs sur les menaces et les attaques numériques existantes ou nouvelles ; leurs stratégies et leurs normes relatives à l'analyse de la vulnérabilité des produits numériques et des stratégies nationales et régionales de gestion des risques et de prévention des conflits, notamment les approches appliquées à l'échelle nationale pour classer les attaques numériques en fonction de leur ampleur et de leur gravité.

84. Les États peuvent également recourir à ces instances pour clarifier leur position et partager volontairement des informations dans les domaines suivants : stratégies nationales en matière de sécurité numérique ; protection des données ; protection des infrastructures critiques tributaires de systèmes informatiques ; mission et fonctions des organismes de sécurité informatique ; stratégie informatique nationale ou organisationnelle ; dispositifs juridiques et systèmes de contrôle qui les régissent.

85. Les recommandations formulées dans les précédents rapports du Groupe d'experts gouvernementaux quant aux mesures de confiance servent de point de départ à une coopération axée sur la lutte contre les menaces croissantes qui pèsent sur les infrastructures critiques, et sur l'application des normes pertinentes. Les États sont encouragés à poursuivre leur travail de sensibilisation quant à l'importance de la protection des infrastructures critiques, à promouvoir les échanges d'informations entre les parties prenantes et à diffuser leurs bonnes pratiques et leurs orientations dans ce domaine. Quand il y a lieu, ils peuvent utiliser les plateformes et les modalités de signalement existantes (voir par. 86) pour communiquer, s'ils le souhaitent, leur position sur la catégorisation des infrastructures nationales critiques et des infrastructures critiques qui fournissent des services essentiels aux niveaux régional ou international, sur la législation et les politiques nationales dans ce domaine, sur les cadres d'évaluation des risques et sur le recensement, la catégorisation et la gestion des attaques numériques ciblant ces infrastructures.

86. Les États pourraient également envisager de mettre à profit les ressources de l'ONU, comme la présentation volontaire de rapports au Secrétaire général, le Cyber Policy Portal, le portail des politiques de cybersécurité de l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR), ainsi que les ressources des autres organisations internationales et régionales compétentes, afin de compiler les informations et les bonnes pratiques que les États ont communiquées sur les stratégies, les politiques, les législations et les programmes nationaux qui portent sur des problématiques de sécurité informatique intéressant la sécurité et la stabilité internationales.

VI. Coopération et assistance internationales en matière de sécurité numérique et de renforcement des capacités

87. Le Groupe d'experts gouvernementaux souligne le rôle essentiel de la coopération et de l'assistance internationales en matière de sécurité numérique et de renforcement des capacités, ainsi que l'importance qu'elles revêtent pour tous les volets de son mandat. L'intensification de la coopération, conjuguée à une assistance plus efficace et à un renforcement des capacités en matière de sécurité numérique associant d'autres parties prenantes, telles que le secteur privé, les universités, la société civile et les milieux techniques, peut aider les États à appliquer le cadre de promotion d'un comportement responsable concernant l'utilisation qu'ils font des technologies numériques. Ces efforts accrus sont essentiels pour combler les fossés qui existent au sein des États et entre eux sur les questions politiques, juridiques et

techniques touchant à la sécurité numérique. Ils peuvent également contribuer à la réalisation d'autres objectifs de la communauté internationale, tels que les objectifs de développement durable.

88. La coopération et l'assistance internationales en matière de sécurité numérique et de renforcement des capacités peuvent accroître la capacité des États de détecter les menaces, d'enquêter sur celles-ci et d'y faire face, et garantir qu'ils soient tous en mesure de faire un usage responsable des technologies numériques. Elles peuvent également contribuer à faire en sorte que les infrastructures critiques de tous les États offrent les niveaux de protection et de sécurité requis, que les États disposent des capacités adéquates en matière de gestion des atteintes à la sécurité informatique et qu'ils puissent demander de l'aide ou répondre à des demandes d'assistance en cas d'attaque numérique émanant de leur territoire ou ciblant celui-ci.

89. Le Groupe d'experts gouvernementaux recommande une consolidation de la coopération et l'assistance internationales en matière de sécurité numérique et de renforcement des capacités, afin d'apporter une aide aux États dans les domaines suivants :

a) L'élaboration et la mise en œuvre de politiques, de stratégies et de programmes relatifs au numérique à l'échelle nationale ;

b) La création et le renforcement des capacités d'intervention des équipes d'intervention informatique d'urgence et des équipes d'intervention en cas d'atteinte à la sécurité informatique, et la consolidation des dispositifs de coopération entre celles-ci ;

c) L'amélioration de la sécurité, de la résilience et de la protection des infrastructures critiques ;

d) Le renforcement ou l'amélioration des capacités techniques, juridiques ou politiques dont disposent les États pour détecter et résoudre les incidents numériques et enquêter à leur sujet, y compris au moyen d'investissements dans le développement des ressources humaines, des institutions, de technologies résilientes et de programmes éducatifs ;

e) Une meilleure compréhension commune de la manière dont le droit international s'applique à l'utilisation des technologies numériques par les États et la promotion de la coopération interétatique, notamment dans le cadre de débats tenus à ce sujet à l'ONU ;

f) Le renforcement des capacités techniques et juridiques de tous les États en matière d'enquête sur les incidents numériques graves et de résolution de ceux-ci ;

g) La mise en œuvre de normes non contraignantes de comportement responsable des États, convenues sur une base volontaire ;

h) À cette fin, et en vue d'évaluer leurs propres priorités, besoins et ressources, les États sont encouragés à utiliser le modèle d'enquête volontaire sur la mise en œuvre nationale recommandé par le Groupe de travail à composition non limitée des Nations Unies[4].

90. Pour combler les fossés numériques et garantir que tous les États bénéficient des retombées des recommandations formulées ci-dessus ainsi que des efforts faits dans d'autres domaines d'assistance et en matière de renforcement des capacités, les États sont encouragés à allouer, dans la mesure du possible, des ressources financières

[4] Rapport de fond final du Groupe de travail à composition non limitée, par. 65.

et des compétences techniques et politiques pour aider les pays qui en font la demande à améliorer leur sécurité numérique.

91. En ce qui concerne l'action que les États mènent en faveur de la coopération et de l'assistance internationales en matière de sécurité numérique et de renforcement des capacités, le Groupe d'experts gouvernementaux souligne le caractère volontaire, politiquement neutre, mutuellement bénéfique et réciproque des activités de renforcement des capacités. À cet égard, il approuve les recommandations du Groupe de travail à composition non limitée en ce qui concerne les principes de renforcement des capacités (processus et finalité, partenariats et personnes) et encourage tous les États à s'en inspirer dans l'action qu'ils mènent pour faire progresser la coopération et l'assistance[5].

92. La promotion de l'émergence de vues communes et de l'apprentissage mutuel peut également renforcer la coopération et l'assistance internationales en matière de sécurité numérique et de renforcement des capacités. Les États devraient réfléchir à des stratégies de coopération multidisciplinaires, multipartites, modulaires et mesurables en matière de sécurité numérique et de renforcement des capacités. Pour cela, ils peuvent collaborer avec l'ONU et d'autres organisations mondiales, régionales et sous-régionales ainsi qu'avec d'autres parties prenantes concernées en vue de faciliter une coordination efficace et la mise en œuvre de programmes de renforcement des capacités et favoriser la transparence et les échanges d'informations concernant l'efficacité de ces programmes.

VII. Conclusions et recommandations pour les travaux futurs

93. Compte tenu de la dépendance croissante des États à l'égard des technologies numériques, il est essentiel d'établir un cadre commun de comportement responsable des États en matière d'utilisation du numérique, conçu sous l'angle de la sécurité internationale, afin que tous les États puissent bénéficier de ces technologies, se prémunir contre leur utilisation abusive et intervenir, le cas échéant.

94. Axant ses efforts sur la promotion d'une vision commune et la mise en œuvre effective des recommandations qu'il a formulées dans ses précédents rapports, le Groupe d'experts gouvernementaux a recensé et précisé les stratégies que les États peuvent adopter afin d'assurer l'efficacité des efforts de coopération entrepris pour faire face aux menaces existantes et potentielles dans le domaine de la sécurité de l'information, et fourni des orientations à cet égard. Ces stratégies sont clairement exposées dans les sections du présent rapport consacrées aux normes, règles et principes volontaires de comportement responsable des États, au droit international, à l'instauration d'un climat de confiance, à la coopération internationale et au renforcement des capacités, qui s'inscrivent toutes dans la continuité des éléments clefs énoncés dans les précédents rapports du Groupe en ce qui concerne le comportement responsable des États.

95. Le Groupe d'experts gouvernementaux a également dressé une liste non exhaustive des domaines d'action sur lesquels pourraient porter les futurs travaux :

a) Renforcer la coopération aux niveaux bilatéral, régional et multilatéral en vue de promouvoir l'adoption de vues communes concernant les menaces existantes et potentielles et les risques qui pourraient peser sur la paix et la sécurité internationales du fait de l'utilisation malveillante des technologies numériques, et concernant la sécurité des infrastructures critiques ;

[5] Rapport de fond final du Groupe de travail à composition non limitée, par. 56.

b) Continuer à partager et à échanger des vues sur les normes, règles et principes volontaires de comportement responsable des États et sur les pratiques nationales et régionales en matière d'application des normes et des mesures de confiance ; poursuivre la définition de la manière dont le droit international s'applique à l'utilisation des technologies numériques par les États, notamment en identifiant des sujets spécifiques de droit international en vue d'un examen plus approfondi ;

c) Intensifier la coopération internationale et le renforcement des capacités en ce qui concerne les évaluations et les recommandations figurant dans le présent rapport, afin que tous les États puissent contribuer au maintien de la paix et de la sécurité internationales, compte tenu du paragraphe 90 ci-dessus ;

d) Recenser des mécanismes favorisant la participation d'autres parties prenantes essentielles, dont le secteur privé, les universités, la société civile et les milieux techniques, aux efforts déployés pour mettre en œuvre le cadre de comportement responsable, lorsque les circonstances s'y prêtent ;

e) Demander à l'UNIDIR, qui propose ses services à tous les États Membres, de réaliser des études pertinentes sur les sujets abordés dans le présent rapport, et encourager d'autres groupes de réflexion et instituts de recherche compétents à faire de même.

96. Le Groupe d'experts gouvernementaux encourage la continuité du processus de négociation inclusif et transparent concernant les technologies numériques dans le contexte de la sécurité internationale organisé sous les auspices des Nations Unies, tenant compte notamment des travaux du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) créé en application de la résolution 75/240 de l'Assemblée générale. Il recommande que les futurs travaux s'appuient sur les travaux accomplis par les groupes d'experts gouvernementaux et le Groupe de travail à composition non limitée.

97. Le Groupe d'experts gouvernementaux encourage les États à poursuivre l'action menée pour développer le cadre de comportement responsable des États au sein de l'Organisation des Nations Unies et d'autres instances régionales et multilatérales, afin de favoriser un dialogue régulier, la concertation et le renforcement des capacités au moyen d'une approche inclusive, fondée sur le consensus, orientée vers l'action et transparente. À cet égard, conformément aux conclusions du Groupe de travail à composition non limitée, il prend note d'une série de propositions visant à promouvoir le comportement responsable des États en matière d'utilisation des technologies numériques et qui renforceraient notamment la capacité des États à honorer les engagements pris en ce qui concerne l'utilisation de ces technologies, en particulier ceux qui sont énoncés dans le Programme d'action. Dans le cadre de l'examen de ces propositions, les préoccupations et les intérêts de tous les États devraient être pris en compte, selon le principe de l'égale participation de tous les États aux processus des Nations Unies. À cet égard, le Programme d'action devrait être étoffé, 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.

98. Le Groupe d'experts gouvernementaux recommande aux États Membres de s'appuyer sur les évaluations et les recommandations figurant dans le présent rapport et dans les rapports établis par les précédents groupes, ainsi que sur les conclusions et les recommandations du rapport final du Groupe de travail à composition non limitée (A/75/816), et d'envisager des moyens de les améliorer et de les mettre en œuvre.

Annexe

Liste des membres du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale

Afrique du Sud
Doc Mashabane
Directeur général du Département de la justice et du développement constitutionnel

Moliehi Makumane (troisième et quatrième sessions)
Conseillère spéciale du représentant de l'Afrique du Sud au sein du Groupe d'experts gouvernementaux

Allemagne
Regine Grienberger (troisième et quatrième sessions)
Ambassadrice pour la cyberpolitique étrangère, Ministère fédéral des affaires étrangères

Wolfram von Heynitz (première et deuxième sessions)
Chef de l'équipe de coordination chargée de la cyberpolitique internationale, Ministère fédéral des Affaires étrangères

Australie
Johanna Weaver
Conseillère spéciale de l'Ambassadeur australien pour les questions de cybersécurité, Département des affaires étrangères et du commerce international

Brésil
Guilherme de Aguiar Patriota
Ambassadeur, Consul général du Brésil à Mumbai

Chine
Wang Lei
Coordinateur pour les questions de cybersécurité, Ministère des affaires étrangères

Estonie
Heli Tiirmaa-Klaar
Ambassadrice itinérante pour la cyberdiplomatie, Directrice générale du Département de la cyberdiplomatie, Ministère des affaires étrangères

États-Unis
Michele Markoff
Coordinatrice par intérim en charge des questions de cybersécurité, Département d'État

Fédération de Russie
Andrey Krutskikh
Représentant spécial du Président de la Fédération de Russie pour la coopération internationale dans le domaine de la sécurité de l'information, Directeur du Département de la sécurité internationale de l'information, Ministère des affaires étrangères

Vladimir Shin (troisième et quatrième sessions)
Directeur adjoint du Département de la sécurité internationale de l'information, Ministère des affaires étrangères

France
Henri Verdier
Ambassadeur pour le numérique, Ministère de l'Europe et des affaires étrangères

Inde
S. Janakiraman
Cosecrétaire et Chef de la Division de la gouvernance en ligne et des technologies de l'information et de la Division de la cyberdiplomatie, Ministère des affaires étrangères

Indonésie
Rolliansyah Soemirat (troisième et quatrième sessions)
Directeur de la sécurité internationale et du désarmement, Ministère des affaires étrangères

Harditya Suryawanto (deuxième session)
Conseiller en charge des questions de cybersécurité, Direction de la sécurité internationale et du désarmement, Ministère des affaires étrangères

Grata Endah Werdaningtyas (première session)
Directrice de la sécurité internationale et du désarmement, Ministère des affaires étrangères

Japon
Takeshi Akahori
Ambassadeur pour les affaires des Nations Unies et la cyberpolitique, Ministère des affaires étrangères

Jordanie
Feras Mohammad Abdallah Alzoubi
Chef de la Division du programme national de cybersécurité, Forces armées jordaniennes

Kazakhstan
Asset Nussupov
Chef de secteur, Cabinet du Président de la République du Kazakhstan

Kenya
Katherine Getao
Administratrice de l'Autorité des technologies de l'information et de la communication

Maroc
Abdellah Boutrig
Colonel-major, Directeur de l'assistance, de la formation, du contrôle et de l'expertise à la Direction générale de la sécurité des systèmes d'information, Administration de la défense nationale

Maurice
Kaleem Ahmed Usmani
Chef de l'équipe d'intervention informatique d'urgence de Maurice (CERT-MU)

Mexique
Gerardo Isaac Morales Tenorio
Coordonnateur en charge de la sécurité multidimensionnelle, Ministère des affaires étrangères

Norvège
Simen Ekblom (troisième et quatrième sessions)
Coordonnateur de la cyberpolitique, Ministère des affaires étrangères

Anniken Krutnes (première et deuxième sessions)
Directrice générale adjointe, Département de la politique de sécurité et du Grand Nord, Ministère des affaires étrangères

Pays-Bas
Carmen Gonsalves
Responsable de la cyberpolitique internationale, Ministère des affaires étrangères

Roumanie
Mihaela-Ionelia Popescu
Coordonnatrice de la cyberpolitique, Ministère des affaires étrangères

Royaume-Uni
Kathryn Jones
Responsable de la cybergouvernance internationale à la Direction nationale de la sécurité, Ministère des affaires étrangères, du Commonwealth et du développement

Alexander Evans (première session)
Ancien Directeur en charge des questions de cybersécurité, Ministère des affaires étrangères, du Commonwealth et du développement

Singapour
David Koh
Directeur général de l'Office de la cybersécurité de Singapour et Commissaire en charge de la cybersécurité

Suisse
Nadine Olivieri Lozano
Ambassadrice, Cheffe de la Division pour la sécurité internationale, Département fédéral des affaires étrangères

Uruguay
Noelia Martínez Franchi (troisième et quatrième sessions)
Directrice des affaires multilatérales, Ministère des affaires étrangères

Alejandra Erramuspe (première et deuxième sessions), membre de l'équipe dirigeante de l'Agence pour l'administration en ligne et la société de l'information, Cabinet du Président