Nations Unies A/75/816

Assemblée générale

Distr. générale
18 mars 2021
Français
Original : anglais

Soixante-quinzième session
Point 98 de l'ordre du jour
Progrès de l'informatique et des télécommunications et sécurité internationale

Progrès de l'informatique et des télécommunications et sécurité internationale

Note du Secrétaire général

Le Secrétaire général a l'honneur de transmettre à l'Assemblée générale le rapport du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, en application de la résolution 73/27 et de la décision 75/550 de l'Assemblée.

21-03673 (F) 140421 140421

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

I. Introduction

1. Par sa résolution 73/27, l'Assemblée générale a décidé de constituer à partir de 2019 un groupe de travail à composition non limitée qui serait chargé, sur la base du consensus, de poursuivre l'élaboration, à titre prioritaire, des règles, normes et principes de comportement responsable des États et de définir des moyens de les appliquer ; d'y apporter des changements ou d'en établir des nouveaux, selon qu'il conviendrait ; d'étudier la possibilité d'instaurer un dialogue institutionnel régulier aussi large que possible sous l'égide de l'Organisation des Nations Unies ; de poursuivre l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité numérique et des mesures de coopération qui pourraient être prises pour y parer, de la manière dont le droit international s'applique à l'utilisation du numérique par les États, ainsi que des mesures de confiance et de renforcement des capacités, en vue de parvenir à une vision commune ; de lui présenter à sa soixante-quinzième session un rapport sur les résultats de cette étude ; d'envisager, dans la limite des contributions volontaires disponibles, la possibilité de tenir des réunions consultatives intersessions avec les parties intéressées, à savoir le secteur privé, les organisations non gouvernementales et les milieux universitaires, pour qu'ils puissent échanger leurs vues sur les questions relevant du mandat du groupe. L'Assemblée a également décidé que le groupe de travail à composition non limitée tiendrait sa session d'organisation en juin 2019 afin de déterminer ses modalités de fonctionnement.

2. Par sa décision 75/550, l'Assemblée générale, notant que, en raison de la pandémie de maladie à coronavirus (COVID-19), la troisième et dernière session de fond prévue du 6 au 10 juillet 2020 avait été annulée, a décidé que le Groupe de travail poursuivrait ses travaux au titre du mandat défini dans la résolution 73/27 et tiendrait sa troisième et dernière session de fond du 8 au 12 mars 2021.

II. Questions d'organisation

A. Ouverture et durée des sessions

3. Le Groupe de travail a tenu sa session d'organisation le 3 juin 2019, sa première session de fond du 9 au 13 septembre 2019, sa deuxième session de fond du 10 au 14 février 2020 et sa troisième session de fond du 8 au 12 mars 2021, toutes au Siège.

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

B. Participation

5. La liste des participantes et participants aux sessions de fond figure dans les documents publiés sous les cotes A/AC.290/2019/INF/1, A/AC.290/2020/INF/1 et A/AC.290/2021/INF/1.

C. Membres du Bureau

6. Lors de sa session d'organisation, le 3 juin 2019, le Groupe de travail a élu par acclamation Juerg Lauber (Suisse) à la présidence.

D. Adoption de l'ordre du jour

7. À la même session, le Groupe de travail a adopté, pour toutes ses sessions, son ordre du jour, tel qu'il figure dans le document publié sous la cote A/AC.290/2019/1. L'ordre du jour se lit comme suit :

1. Élection du Bureau.
2. Adoption de l'ordre du jour.
3. Organisation des travaux.
4. Échange de vues général.
5. Débats sur les questions de fond mentionnées au paragraphe 5 de la résolution 73/27 de l'Assemblée générale :
    a) Poursuite de l'élaboration des règles, normes et principes de comportement responsable des États visés au paragraphe 1 de ladite résolution et définition des moyens de les appliquer ; modification de ceux-ci ou établissement de nouvelles règles, selon qu'il conviendra ;
    b) Étude de la possibilité d'instaurer un dialogue institutionnel régulier aussi large que possible sous l'égide de l'Organisation des Nations Unies ;
    c) Poursuite de l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité numérique et des mesures de coopération qui pourraient être prises pour y parer, en vue de parvenir à une vision commune ;
    d) Manière dont le droit international s'applique à l'utilisation du numérique par les États ;
    e) Mesures de confiance ;
    f) Mesures de renforcement des capacités, et principes visés au paragraphe 3 de ladite résolution.
6. Questions diverses.
7. Adoption du rapport final.

8. Toujours à la même session, le Groupe de travail a décidé de mener ses travaux en appliquant le règlement intérieur des grandes commissions de l'Assemblée générale, et sur la base du consensus, conformément à la résolution 73/27 de l'Assemblée. Il a également décidé que, conformément au Règlement intérieur et à la pratique antérieure de l'Assemblée, tous les États Membres auraient le droit d'être représentés au sein du Groupe. Les États non membres, les organisations intergouvernementales et les entités auxquelles le statut d'observateur a été octroyé par l'Assemblée seraient invités à participer aux sessions et aux travaux du Groupe en leur qualité d'observateurs. Les entités compétentes du système des Nations Unies seraient également invitées à participer à des fins d'information technique uniquement. En outre, les organisations non gouvernementales compétentes dotées du statut consultatif auprès du Conseil économique et social conformément à la

résolution 1996/31 feraient part au secrétariat du Groupe de leur intérêt à participer à ses travaux. Les autres organisations non gouvernementales compétentes intéressées par la portée et l'objectif des travaux du Groupe informeraient également le secrétariat du Groupe de leur intérêt et seraient par conséquent invitées à participer, en leur qualité d'observatrices, selon la procédure d'approbation tacite.

E. Organisation des travaux

9. À la première séance de chaque session de fond, les 9 septembre 2019, 10 février 2020 et 8 mars 2021, respectivement, le Groupe de travail a convenu de l'organisation de ses travaux telle qu'elle figurait dans les documents portant les cotes A/AC.290/2019/2, A/AC.290/2020/1 et A/AC.290/2021/1.

F. Documentation

10. Une liste complète de tous les documents officiels, documents de travail, documents techniques et autres documents dont était saisi le Groupe de travail est disponible sur le site Web suivant : www.un.org/disarmament/open-ended-working-group/.

G. Activités du Groupe de travail

11. À sa première session de fond, le Groupe de travail a examiné les points 3 à 5 de l'ordre du jour lors de ses neuf séances plénières.

12. À sa deuxième session de fond, le Groupe de travail a poursuivi l'examen du point 5 de l'ordre du jour durant ses neuf séances plénières.

13. À sa troisième session de fond, le Groupe de travail a examiné les points 5 à 7 de l'ordre du jour.

14. Afin de poursuivre ses travaux pendant la pandémie de maladie à coronavirus (COVID-19), le Groupe de travail a tenu des réunions à distance informelles, les 15, 17 et 19 juin et le 2 juillet 2020 ; du 29 septembre au 1er octobre 2020 ; du 17 au 19 novembre 2020 ; du 1er au 3 décembre 2020 et les 18, 19 et 22 février 2021.

15. Le Groupe de travail a tenu, entre sessions, une réunion consultative informelle multipartite du 2 au 4 décembre 2019. À la demande du Président du Groupe, la réunion a été présidée par le Directeur de la Cyber Security Agency de Singapour, David Koh, dont le résumé des travaux a été présenté et distribué aux membres du Groupe[1].

III. Adoption du rapport

16. À sa troisième session de fond, le 12 mars 2021, le Groupe de travail a examiné le point 7 de l'ordre du jour, intitulé « Adoption du rapport », et a adopté son rapport tel qu'il figurait dans les documents portant les cotes A/AC.290/2021/L.1, tel que révisé oralement, et A/AC.290/2021/CRP.2.

17. Compte tenu des restrictions liées à la COVID-19 en vigueur au Siège de l'Organisation des Nations Unies, qui ont limité le nombre des séances du groupe de travail à sa troisième session de fond, un recueil des déclarations visant à expliquer la position des États sera publié sous la cote A/AC.290/2021/INF.2.

[1] Consultable à l'adresse suivante : www.un.org/disarmament/open-ended-working-group/.

Annexe I*

Rapport de fond final

A. Introduction

1. Malgré les transformations radicales que le monde a connues depuis qu'elle a été créée il y a 75 ans, le but et les idéaux intemporels de l'Organisation des Nations Unies conservent leur pertinence fondamentale. Parallèlement à la réaffirmation de leur foi dans les droits fondamentaux de l'homme et à l'engagement qu'ils ont pris de favoriser le progrès économique et social de tous les peuples et de créer les conditions nécessaires à la justice et au respect du droit international, les États ont pris la résolution d'unir leurs forces pour maintenir la paix et la sécurité internationales[2].

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

3. La nécessité impérieuse d'établir et de préserver, au niveau international, la paix, la sécurité, la coopération et la confiance dans l'environnement numérique est plus évidente que jamais. Les tendances négatives dans le domaine numérique pourraient compromettre la sécurité et la stabilité internationales, exercer des pressions sur la croissance économique et le développement durable et entraver la pleine jouissance des droits humains et des libertés fondamentales. Il s'agit notamment de l'utilisation croissante des TIC à des fins malveillantes.

4. La crise sanitaire mondiale actuelle a mis en évidence les avantages fondamentaux des TIC et notre dépendance à leur égard, notamment pour ce qui est des services publics cruciaux, de la communication de messages essentiels de sécurité publique, de l'élaboration de solutions innovantes pour assurer la continuité des activités, de l'accélération de la recherche, de la continuité de l'enseignement et de la contribution au maintien de la cohésion sociale par des moyens virtuels. En cette période d'incertitude, les États, ainsi que le secteur privé, les chercheurs et d'autres acteurs, ont tiré parti de la technologie numérique pour maintenir les individus et les sociétés en contact et en bonne santé. Dans le même temps, la pandémie de COVID-19 a mis en évidence les risques et les conséquences des activités malveillantes visant à exploiter les vulnérabilités à un moment où les sociétés sont soumises à d'énormes pressions. Elle a également fait ressortir la nécessité de combler les fossés numériques, de renforcer la résilience de chaque société et de chaque secteur et de maintenir une approche centrée sur l'être humain.

5. Comme les TIC peuvent être utilisées à des fins incompatibles avec l'objectif du maintien de la paix, de la stabilité et de la sécurité internationales, l'Assemblée générale a reconnu[3] que la diffusion et l'emploi des technologies et moyens informatiques intéressent la communauté internationale tout entière et qu'une vaste coopération internationale contribuera à une efficacité optimale.

6. À la lumière de ce qui précède, le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale créé par la résolution 73/27 de l'Assemblée générale a donné

---

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

[2] Préambule de la Charte des Nations Unies.

[3] Voir, par exemple, A/RES/53/70, sixième alinéa du préambule.

l'occasion d'examiner plus avant cette question cruciale. Il a offert une tribune démocratique, transparente et inclusive à tous les États pour participer, exprimer leurs points de vue et étendre la coopération pour ce qui a trait au volet sécurité internationale des TIC. La participation active des Membres de l'Organisation des Nations Unies et la mobilisation de diverses autres parties prenantes démontrent l'intérêt collectif de la communauté internationale et son aspiration générale à un environnement numérique pacifique et sûr pour tous, ainsi que sa détermination à coopérer pour y parvenir.

7. La création du Groupe de travail est une étape importante en matière de coopération internationale en vue de l'instauration d'un environnement numérique ouvert, sûr, stable, accessible et pacifique. À six reprises depuis 2003, des groupes d'experts gouvernementaux ont été chargés d'étudier les menaces qui se posent ou pourraient se poser dans le domaine de la sécurité numérique, et les mesures de coopération qui pourraient être prises pour y faire face[4]. Dans leurs trois rapports de consensus (2010, 2013 et 2015[5]), qui sont cumulatifs par nature, ces groupes ont recommandé 11 normes facultatives et non contraignantes de comportement responsable des États et pris en considération le fait que des normes supplémentaires pourraient être élaborées au fil du temps. En outre, des mesures spécifiques de confiance, de renforcement des capacités et de coopération ont été recommandées. Les groupes d'experts ont par ailleurs réaffirmé que le droit international, en particulier la Charte des Nations Unies, était applicable et essentiel pour maintenir la paix, la sécurité et la stabilité dans l'environnement numérique. Dans la résolution 70/237 de l'Assemblée générale, les États Membres ont convenu par consensus de s'inspirer, pour ce qui touchait à l'utilisation de l'informatique et des technologies des communications, du rapport de 2015 du Groupe d'experts gouvernementaux, établissant ainsi plus solidement un premier cadre de comportement responsable des États en matière d'utilisation des TIC. À cet égard, le Groupe de travail a également pris note des résolutions 73/27 et 73/266 de l'Assemblée générale.

8. Sur cette base, réaffirmant le cadre établi, le Groupe de travail a cherché à trouver un terrain d'entente et à assurer la compréhension mutuelle entre tous les États Membres de l'Organisation des Nations Unies quant à un sujet d'importance mondiale. Conformément à son mandat, le Groupe de travail a étudié les menaces qui se posent ou pourraient se poser dans le domaine de la sécurité numérique, et les mesures de coopération qui pourraient être prises pour y faire face ; l'élaboration d'autres normes, règles et principes de comportement responsable des États ; la manière dont le droit international s'applique à l'utilisation des TIC par les États ; les mesures de confiance ; le renforcement des capacités ; et la possibilité d'instaurer un dialogue institutionnel régulier aussi large que possible sous l'égide de l'Organisation des Nations Unies. Afin d'établir un consensus et de promouvoir la paix, la sécurité, la coopération et la confiance au niveau international, les discussions du Groupe de travail ont été guidées par les principes d'inclusivité et de transparence.

9. L'Organisation des Nations Unies devrait continuer de jouer un rôle moteur pour ce qui est de promouvoir le dialogue sur l'utilisation des TIC par les États. Le Groupe de travail reconnaît l'importance et la complémentarité des discussions d'experts relatives à certains aspects des technologies numériques tenues dans d'autres organes et instances des Nations Unies.

10. Si les États sont responsables au premier chef du maintien de la paix et de la sécurité internationales, toutes les parties prenantes ont la responsabilité d'utiliser les TIC d'une manière qui ne mette pas en danger la paix et la sécurité. Comme la dimension sécurité internationale des TIC recoupe de multiples domaines et

[4] A/RES/58/32, A/RES/60/45, A/RES/66/24, A/RES/68/243, A/RES/70/237, A/RES/73/266.
[5] A/65/201, A/68/98 et A/70/174.

disciplines, le Groupe de travail a bénéficié de l'expertise, des connaissances et de l'expérience partagées par les représentants des organisations intergouvernementales, des organisations régionales, de la société civile, du secteur privé, des universités et de la communauté technique. La réunion consultative informelle de trois jours qu'il a tenue en décembre 2019 a donné lieu à une riche discussion entre les États et d'autres parties prenantes très diverses[6]. Ces parties prenantes ont en outre présenté des propositions concrètes et des exemples de bonnes pratiques dans des contributions écrites et lors d'échanges informels avec le Groupe de travail. Certaines délégations ont également mené de leur propre initiative des consultations multipartites afin d'éclairer leurs contributions au Groupe de travail.

11. Ayant à l'esprit que les situations, les capacités et les priorités des États et des régions sont différentes, le Groupe de travail est conscient que les avantages des technologies numériques ne sont pas répartis de manière égale et que la réduction des fractures numériques, notamment grâce à un accès universel, inclusif et non discriminatoire aux TIC et à la connectivité, reste une priorité urgente pour la communauté internationale.

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

13. Le Groupe de travail souligne que les différents éléments qui composent son mandat sont interdépendants et se renforcent mutuellement, et qu'ensemble, ils favorisent un environnement numérique ouvert, sûr, stable, accessible et pacifique.

B. Conclusions et recommandations

14. Après avoir examiné les aspects de fond du mandat du Groupe de travail, et rappelant que, dans sa résolution 73/27, l'Assemblée générale s'est félicitée de l'efficacité des travaux réalisés en 2010, 2013 et 2015 par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale ainsi que des rapports auxquels ils ont abouti, qui lui ont été transmis par le Secrétaire général[7], les États sont parvenus aux conclusions et recommandations suivantes, qui prévoient des actions concrètes et des mesures de coopération pour faire face aux menaces liées aux TIC et promouvoir un environnement numérique ouvert, sûr, stable, accessible et pacifique.

Menaces existantes et potentielles

15. Les États ont conclu qu'ils étaient de plus en plus préoccupés par les conséquences de l'utilisation malveillante des TIC pour le maintien de la paix et de la sécurité internationales, et par la suite pour les droits humains et le développement. Des préoccupations ont notamment été exprimées concernant le développement de capacités informatiques à des fins qui compromettent la paix et la sécurité internationales. Les incidents informatiques préjudiciables sont de plus en plus

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

[7] A/65/201, A/68/98 et A/70/174.

fréquents et sophistiqués, et ne cessent d'évoluer et de se diversifier. L'augmentation de la connectivité et du recours aux TIC, sans mesures de sécurité adaptées, peut entraîner des risques imprévus, rendant les sociétés plus vulnérables aux activités informatiques malveillantes. En dépit des avantages inestimables des technologies de l'information et des communications pour l'humanité, leur utilisation à des fins malveillantes peut avoir des répercussions négatives considérables et de grande envergure.

16. Des États ont rappelé qu'un certain nombre d'États développaient des capacités dans ce domaine à des fins militaires. Ils ont également rappelé qu'il était de plus en plus probable que les TIC soient utilisées dans des conflits futurs entre États. L'augmentation constante du nombre d'incidents impliquant l'utilisation malveillante des technologies de l'information et des communications par des acteurs étatiques et non étatiques, y compris des terroristes et des groupes criminels, était une tendance inquiétante. Certains acteurs non étatiques avaient montré qu'ils possédaient des capacités en matière de TIC qui n'étaient auparavant accessibles qu'aux États.

17. Les États ont également conclu que toute utilisation des TIC par les États d'une manière incompatible avec les obligations qui leur incombent en vertu du cadre établi, qui comprend des normes facultatives, le droit international et des mesures de confiance, compromet la paix et la sécurité internationales, la confiance et la stabilité entre les États, et est susceptible d'accroître la probabilité de conflits futurs entre États.

18. Les États ont conclu que les attaques informatiques contre des infrastructures critiques et des infrastructures d'information critiques servant à fournir des services essentiels au public pouvaient avoir des conséquences dévastatrices sur la sécurité, l'économie et la société, ainsi que sur le plan humanitaire. Bien qu'il appartienne à chaque État de déterminer les infrastructures qu'il considère comme critiques, ces dernières peuvent inclure des établissements médicaux, des établissements financiers et des infrastructures liées à l'énergie, à l'eau, aux transports et à l'assainissement. Les attaques contre les infrastructures critiques et les infrastructures d'information critiques qui sapent la confiance dans les processus politiques et électoraux et dans les institutions publiques, ou qui ont un impact sur la disponibilité ou l'intégrité d'Internet, sont également une préoccupation réelle et croissante. Ces infrastructures peuvent être détenues, gérées ou exploitées par le secteur privé, partagées ou mises en réseau avec un autre État ou encore exploitées dans différents États. En conséquence, la coopération interétatique ou entre le secteur public et le secteur privé peut être nécessaire pour en protéger l'intégrité, le fonctionnement et l'accès.

19. Les États ont également conclu que les activités numériques contraires aux obligations découlant du droit international qui endommagent intentionnellement des infrastructures critiques ou compromettent l'utilisation et le fonctionnement d'infrastructures essentielles à la fourniture de services au public, pourraient constituer une menace non seulement pour la sécurité, mais aussi pour la souveraineté des États, ainsi que pour le développement économique et les moyens de subsistance et, en définitive, pour la sécurité et le bien-être des personnes.

20. Tous les États étant de plus en plus dépendants des technologies numériques, les États ont conclu qu'un manque d'information et de capacités s'agissant de détecter les attaques informatiques, de s'en défendre ou d'y répondre pouvait les rendre plus vulnérables. Comme l'a montré l'actuelle urgence sanitaire mondiale, les vulnérabilités existantes peuvent être amplifiées en temps de crise.

21. Les États ont conclu qu'ils pouvaient vivre différemment les menaces en fonction de leurs niveaux de numérisation et de capacité, de la sécurité et de la résilience de leurs technologies de l'information et des communications, de leur

infrastructure et de leur développement. Les menaces pouvaient également avoir un impact différent sur différents groupes et entités, notamment sur les jeunes, les personnes âgées, les femmes et les hommes, les personnes vulnérables, certaines professions et les petites et moyennes entreprises, entre autres.

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

23. Les États ont souligné les possibilités économiques et sociales positives liées aux TIC et conclu que c'était l'utilisation abusive de ces technologies, et non les technologies elles-mêmes, qui était préoccupante.

Normes, règles et principes relatifs au comportement responsable des États

24. Les normes facultatives et non contraignantes de comportement responsable des États peuvent permettre de réduire les risques pour la paix, la sécurité et la stabilité internationales, et jouer un rôle important pour ce qui est d'accroître la prévisibilité et de réduire le risque d'erreurs d'interprétation, contribuant ainsi à la prévention des conflits. Les États ont souligné que ces normes reflétaient les attentes et les exigences de la communauté internationale s'agissant de l'utilisation des TIC par les États, et qu'elles permettaient à la communauté internationale d'évaluer les activités des États. Conformément à la résolution 70/237 de l'Assemblée générale, et compte tenu de la résolution 73/27 de l'Assemblée générale, les États ont été invités à éviter et à s'abstenir d'utiliser des TIC de manière non conforme aux normes de comportement responsable des États.

25. Les États ont réaffirmé que les normes ne remplaçaient ni ne modifiaient les obligations des États en vertu du droit international, lesquelles étaient contraignantes, ni même leurs droits, mais fournissaient plutôt des orientations spécifiques supplémentaires sur ce qui constituait un comportement responsable de l'État dans l'utilisation des TIC. Ces normes ne cherchaient pas à limiter ou à interdire des actes qui respectaient le droit international.

26. Tout en convenant de la nécessité de protéger toutes les infrastructures critiques et les infrastructures d'information critiques qui servent à fournir des services essentiels au public, et de s'efforcer de garantir la disponibilité générale et l'intégrité d'Internet, les États ont également conclu que la pandémie de COVID-19 avait rendue plus importante encore la protection des infrastructures de soins de santé, notamment les services et les établissements médicaux, par l'application de normes spécifiques telles que celles énoncées dans la résolution 70/237 de l'Assemblée générale de l'Organisation des Nations Unies, qui font l'objet d'un consensus.

27. Les États ont affirmé l'importance de soutenir et de poursuivre les efforts visant à mettre en œuvre aux niveaux mondial, régional et national des normes que les États s'engageaient à respecter.

28. Les États, réaffirmant la résolution 70/237 de l'Assemblée générale et prenant acte de sa résolution 73/27, devraient prendre des dispositions raisonnables pour garantir l'intégrité de la chaîne d'approvisionnement, notamment en adoptant des mesures de coopération objectives, de sorte que les utilisateurs finaux puissent avoir confiance dans la sécurité des produits numériques ; s'attacher à prévenir la

prolifération des techniques et des outils informatiques malveillants et l'utilisation de fonctionnalités cachées malveillantes ; encourager le signalement responsable des failles.

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

Le Groupe de travail recommande que :

30. Les États, à titre volontaire, passent en revue les efforts faits au niveau national pour mettre en œuvre les normes et étoffer leurs expériences et leurs bonne pratiques à cet égard et les partager et continuent à tenir le Secrétaire général informé de leurs vues et de leurs observations nationales sur le sujet.

31. Les États ne mènent ni ne soutiennent sciemment une activité numérique qui est contraire aux obligations qu'ils ont contractées en vertu du droit international et qui endommage intentionnellement des infrastructures essentielles ou qui compromet l'utilisation et le fonctionnement d'infrastructures essentielles à la fourniture de services au public, et qu'ils continuent en outre à renforcer les mesures visant à garantir toutes les infrastructures critiques contre les menaces liées aux TIC et multiplier les échanges concernant les bonnes pratiques relatives à la protection de ces infrastructures.

32. Les États, en partenariat avec les organisations concernées, notamment l'Organisation des Nations Unies, encouragent plus avant la mise en œuvre et le développement par tous les États de normes de comportement responsable, et que les États en mesure d'apporter à cet égard leur expertise et leurs ressources soient encouragés à le faire.

33. Les États, ayant à l'esprit la résolution 70/237 de l'Assemblée générale et prenant acte de sa résolution 73/27, prennent note des propositions que les États formuleront concernant l'enrichissement des normes, règles et principes de comportement responsable des États dans le cadre des discussions sur les TIC qui seront organisées au sein du système des Nations Unies, notant que l'Assemblée a créé, par sa résolution 75/240, un Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

Droit international

34. Tenant compte de la résolution 70/237 de l'Assemblée générale et prenant acte de sa résolution 73/27, par laquelle a été créé le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications, les États ont réaffirmé que le droit international, en particulier la Charte des Nations Unies, était applicable et essentiel au maintien de la paix et de la stabilité et à la création d'un environnement numérique ouvert, sûr, stable, accessible et pacifique. À cet égard, les États ont été invités à s'abstenir de prendre des mesures dérogeant au droit international et en particulier à la Charte des Nations Unies. Les États ont également conclu qu'il fallait promouvoir une meilleure compréhension commune de la manière dont le droit international s'appliquait à leur utilisation des TIC.

35. Les États ont réaffirmé qu'ils devaient s'employer à régler les différends par des moyens pacifiques tels que la négociation, l'enquête, la médiation, la conciliation, l'arbitrage, le règlement judiciaire et le recours aux organismes ou accords régionaux, ou par d'autres moyens pacifiques de leur choix.

36. Les États ont conclu que compte tenu de la spécificité de l'environnement numérique, il était possible d'approfondir la compréhension commune de la manière dont le droit international s'appliquait à leur utilisation des TIC en échangeant des vues sur la question et en identifiant des sujets spécifiques de droit international en vue d'un examen plus approfondi au sein du système des Nations Unies.

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

Le Groupe de travail recommande que :

38. Les États, à titre volontaire, continuent de faire part au Secrétaire général de leurs vues et de leurs observations nationales quant à la manière dont le droit international s'applique à leur utilisation des technologies numériques dans le contexte de la sécurité internationale, et continuent de communiquer volontairement des informations sur ces vues et sur leurs pratiques nationales par d'autres moyens appropriés.

39. Les États qui sont en mesure de le faire continuent de soutenir, de manière neutre et objective, les efforts supplémentaires visant à renforcer les capacités, conformément aux principes énoncés au paragraphe 56 du présent rapport, dans les domaines du droit international, de la législation nationale et de l'élaboration des politiques, afin que tous les États contribuent à forger une compréhension commune de la manière dont le droit international s'applique à l'utilisation des technologies numériques par les États, et de contribuer à l'instauration d'un consensus au sein de la communauté internationale.

40. Les États continuent d'étudier la manière dont le droit international s'applique à l'utilisation des TIC par les États et de l'examiner dans le cadre de futurs processus des Nations Unies, ce qui est essentiel pour clarifier la question et en développer une meilleure compréhension commune.

Mesures de confiance

41. Les mesures de confiance, qui incluent des mesures de transparence, de coopération et de stabilité, peuvent contribuer à la prévention des conflits ainsi qu'à permettre d'éviter les erreurs d'interprétation et les malentendus et de réduire les tensions. Elles sont une expression concrète de la coopération internationale. Accompagnées des ressources, des capacités et de la volonté nécessaires, les mesures de confiance peuvent renforcer la sécurité, la résilience et l'utilisation pacifique des TIC. Elles peuvent également étayer la mise en œuvre de normes de comportement responsable des États, dans la mesure où elles favorisent la confiance et assurent une plus grande clarté, prévisibilité et stabilité dans l'utilisation des TIC par les États. Avec les autres piliers du cadre de comportement responsable des États, les mesures de confiance peuvent également contribuer à l'instauration d'une communauté de vues entre les États, contribuant ainsi à un environnement international plus pacifique.

42. Comme les mesures de confiance sont des engagements volontaires pris progressivement, elles peuvent constituer une première étape pour dissiper la méfiance que des malentendus pourraient faire naître entre les États en établissant la communication, en jetant des ponts et en suscitant la coopération autour d'un objectif

commun présentant un intérêt mutuel. En tant que telles, ces mesures peuvent poser les bases d'accords et d'arrangements élargis, supplémentaires ou plus structurés dans l'avenir.

43. Les États ont conclu que le dialogue au sein du Groupe de travail était en soi une mesure de confiance, car il stimulait un échange de vues ouvert et transparent sur la perception des menaces et des vulnérabilités, le comportement responsable des États et d'autres acteurs et les bonnes pratiques, ce qui, en fin de compte, encourageait l'élaboration et la mise en œuvre collectives du cadre de comportement responsable des États en matière d'utilisation des TIC.

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

45. S'appuyant sur les atouts essentiels que sont la confiance et les relations établies, les États ont reconnu que les organisations régionales et sous-régionales avaient déployé des efforts considérables pour élaborer des mesures de confiance, les adapter à leurs besoins et à leurs priorités spécifiques, sensibiliser l'opinion publique et partager l'information entre leurs membres. En outre, les échanges régionaux, interrégionaux et interorganisations peuvent ouvrir de nouvelles perspectives en matière de collaboration, de coopération et d'apprentissage mutuel. Du fait que tous les États ne sont pas membres d'une organisation régionale et que toutes les organisations régionales n'ont pas mis en place des mesures de confiance, il a été noté que ces mesures étaient complémentaires de l'action menée par l'ONU et par d'autres organisations pour promouvoir les mesures de confiance.

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

47. Concrètement, les États ont conclu que la désignation d'interlocuteurs nationaux était une mesure de confiance en soi, mais qu'elle était également utile à la mise en œuvre de nombreuses autres mesures de confiance, et qu'elle avait une valeur inestimable en temps de crise. Les États pourront trouver utile de se doter d'interlocuteurs aux fins, entre autres, des échanges diplomatiques, politiques, juridiques et techniques, ainsi que pour le signalement des incidents et les interventions.

Le Groupe de travail recommande que :

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

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

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

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

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

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

Renforcement des capacités

54. La capacité de la communauté internationale de prévenir ou d'atténuer l'impact d'activités malveillantes dans le domaine des TIC dépend de la capacité de chaque État de se préparer et de réagir. Cette question revêt encore plus d'importance pour les pays en développement, l'objectif étant de faciliter leur participation véritable aux discussions sur les TIC dans le contexte de la sécurité internationale et les aider à corriger les vulnérabilités de leurs infrastructures critiques. Le renforcement des capacités contribue à mettre en valeur les compétences, les ressources humaines, les politiques et les institutions qui accroissent la résilience et la sécurité des États afin qu'ils puissent bénéficier pleinement des technologies numériques. Il joue un rôle important dans la promotion de l'adhésion au droit international et la mise en œuvre des normes de comportement responsable des États et dans l'appui à la mise en œuvre des mesures de confiance. Dans un monde numériquement interdépendant, les avantages du renforcement des capacités rayonnent au-delà des bénéficiaires initiaux et contribuent à la création d'un environnement numérique plus sûr et plus stable pour tous.

55. Garantir un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies numériques exige que les États coopèrent efficacement en vue de réduire les risques pour la paix et la sécurité internationales. Le renforcement des capacités est un aspect important de cette coopération et constitue un acte volontaire de la part du donateur aussi bien que du bénéficiaire.

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

Processus et finalité

• Le renforcement des capacités doit être un processus durable, prévoyant l'exécution d'activités spécifiques par et pour différents acteurs.

• Ces activités spécifiques doivent avoir une finalité claire et être axées sur les résultats, tout en tendant vers l'objectif commun d'un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies numériques.

• Les activités de renforcement des capacités doivent reposer sur des données factuelles, être politiquement neutres, transparentes, responsables et ne faire l'objet d'aucune condition.

• Le renforcement des capacités doit être entrepris dans le plein respect du principe de la souveraineté des États.

• Il peut être nécessaire de faciliter l'accès aux technologies pertinentes.

Partenariats

• Le renforcement des capacités doit être fondé sur la confiance mutuelle, être axé sur la demande, correspondre aux besoins et priorités identifiés au niveau national et être entrepris en toute reconnaissance de l'appropriation nationale. Les partenaires du renforcement des capacités participent à titre volontaire.

• Les activités de renforcement des capacités devant être adaptées à des besoins et à des contextes spécifiques, toutes les parties sont des partenaires actifs aux responsabilités partagées mais différenciées, s'agissant notamment de collaborer à la conception, à l'exécution, au suivi et à l'évaluation des activités en question.

• La confidentialité des politiques et des plans nationaux doit être protégée et respectée par tous les partenaires.

Personnes

• Le renforcement des capacités doit être respectueux des droits humains et des libertés fondamentales, tenir compte des questions de genre et être inclusif, universel et non discriminatoire.

• La confidentialité des informations sensibles doit être garantie.

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

58. Les États ont conclu que le renforcement des capacités devait contribuer à transformer le fossé numérique en opportunités numériques et devait servir en particulier à faciliter la participation véritable des pays en développement aux débats et forums sur la question et à renforcer la résilience de ces pays dans l'environnement numérique.

59. Les États ont conclu que le renforcement des capacités pouvait contribuer à favoriser la compréhension et la prise en compte des risques systémiques et autres découlant d'une sécurité numérique déficiente, d'une coordination insuffisante entre les capacités techniques et politiques au niveau national et des problèmes connexes que constituaient les inégalités et les fractures numériques. Le renforcement des capacités visant à permettre aux États de recenser et de protéger les infrastructures

nationales critiques et d'œuvrer en coopération à la préservation des infrastructures d'information critiques a été jugé particulièrement important. Le renforcement des capacités peut également aider les États à mieux comprendre la manière dont le droit international s'applique. Le partage et la coordination des informations aux niveaux national, régional et international peuvent rendre les activités de renforcement des capacités plus efficaces, plus stratégiques et plus conformes aux priorités nationales.

60. Au-delà des compétences techniques, du renforcement des institutions et des mécanismes de coopération, les États ont conclu qu'il était urgent d'acquérir des compétences spécialisées dans toute une série de domaines à caractère diplomatique, juridique, décisionnel, législatif et réglementaire. Dans ce contexte, l'importance de développer les capacités diplomatiques pour s'engager dans des processus internationaux et intergouvernementaux a été soulignée.

61. Les États ont rappelé la nécessité d'une approche du renforcement des capacités qui soit concrète et orientée vers l'action. Ils ont conclu que des mesures concrètes pourraient inclure un soutien aux niveaux décisionnel et technique recouvrant par exemple l'élaboration de stratégies nationales de cybersécurité, l'octroi d'un accès aux technologies pertinentes, le soutien aux équipes d'intervention rapide dans le domaine informatique ou aux équipes d'intervention en cas d'atteinte à la sécurité informatique et la mise en place de formations spécialisées et de programmes d'études adaptés, y compris des programmes de « formation des formateurs » et de certification professionnelle. L'utilité de créer des plateformes d'échange d'information, notamment concernant les bonnes pratiques juridiques et administratives, a été reconnue, de même que la valeur des contributions apportées par d'autres parties prenantes aux activités de renforcement des capacités.

62. Les États ont conclu qu'il était utile de faire le bilan de l'action menée au niveau national pour donner suite aux conclusions et recommandations formulées dans le présent rapport ainsi qu'aux observations et recommandations sur lesquelles ils étaient convenus de se fonder, selon la résolution 70/237, afin d'évaluer les progrès accomplis et de repérer les domaines dans lesquels les capacités devaient encore être renforcées.

Le Groupe de travail recommande que :

63. Les États soient guidés par les principes énoncés au paragraphe 56 du présent rapport dans leurs efforts de renforcement des capacités liées aux TIC dans le domaine de la sécurité internationale et que les autres intervenants soient encouragés à tenir compte de ces principes dans leurs propres activités de renforcement de capacités.

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

65. Les États, à titre volontaire, s'appuient à cet effet sur le modèle d'enquête nationale sur la mise en œuvre de la résolution 70/237 de l'Assemblée générale des Nations Unies (« National Survey of Implementation of United Nations General Assembly Resolution 70/237 ») (qui sera publié en ligne). Les États Membres pourront également souhaiter utiliser volontairement le modèle d'enquête pour structurer la présentation des informations qu'ils communiqueront au Secrétaire général sur leurs vues et observations.

66. Les États et autres acteurs qui sont en mesure d'offrir une aide financière, en nature ou technique en faveur du renforcement des capacités soient encouragés à le

faire. Il conviendrait de faciliter davantage la coordination et le financement des efforts de renforcement des capacités, notamment entre les organisations concernées et l'Organisation des Nations Unies.

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

Dialogue institutionnel régulier

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

69. Au-delà de chercher à trouver un terrain d'entente entre tous les États grâce à des échanges constructifs, le Groupe de travail a favorisé les réseaux diplomatiques et cultivé la confiance entre les participants. La large participation de parties prenantes non gouvernementales a démontré qu'une communauté d'acteurs plus vaste était prête à tirer parti de son expertise pour aider les États à atteindre leur objectif de garantir un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies numériques. Les travaux du Groupe de travail ont confirmé l'importance de discussions récurrentes et structurées sous les auspices des Nations Unies au sujet de l'utilisation des TIC.

70. Les États ont conclu qu'un dialogue suivi sous les auspices des Nations Unies favorisait la réalisation des objectifs communs que sont le renforcement de la paix et de la stabilité internationale et la prévention des conflits dans l'environnement numérique. Ils ont également conclu qu'au vu de la dépendance croissante à l'égard des TIC et l'ampleur des menaces émanant de leur utilisation malveillante, il était urgent de continuer à renforcer les positions communes, d'instaurer la confiance et d'intensifier la coopération internationale.

71. Les États ayant la responsabilité première du maintien de la sécurité nationale, de la sûreté publique et de l'état de droit, ils ont affirmé qu'il importait de maintenir un dialogue intergouvernemental suivi et de définir des mécanismes appropriés de collaboration avec d'autres groupes de parties prenantes dans le cadre de processus futurs.

72. L'examen à l'ONU des progrès de l'informatique et des communications dans le contexte de la sécurité internationale met l'accent sur les aspects liés à la paix et à la stabilité internationales et à la prévention des conflits. Les États ont conclu que le dialogue institutionnel régulier qui aurait lieu à l'avenir ne devrait pas faire double emploi avec les mandats, efforts et activités déjà mis en place par l'Organisation concernant la dimension numérique d'autres questions[8]. Les États ont conclu qu'un échange accru entre les instances chargées de ces efforts et les processus établis par la Première Commission pourrait contribuer à renforcer les synergies et à améliorer la cohérence, tout en respectant les compétences ou le mandat spécialisé de chaque organe.

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

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

vues ne s'est encore dégagée. Les États ont constaté qu'il était utile de réfléchir à des moyens de suivre l'élaboration de nouvelles règles et normes et l'application de celles qui ont déjà été convenues.

74. Les États ont conclu que tout futur processus de dialogue institutionnel régulier mis en place sous les auspices des Nations Unies devrait être orienté vers l'action et assorti d'objectifs spécifiques, élargir la portée des réalisations précédentes et être inclusif, transparent, fondé sur le consensus et axé sur les résultats.

Le Groupe de travail recommande que :

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

76. Les États assurent la continuité du processus de négociation inclusif et transparent concernant les TIC 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.

77. Les États prennent note d'une série de propositions visant à promouvoir le comportement responsable des États en matière de TIC et qui renforceraient notamment la capacité des États à honorer les engagements qu'ils ont pris en matière d'utilisation des TIC, 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.

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

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

C. Observations finales

80. Les États ont participé de manière régulière et active à l'ensemble des travaux du Groupe de travail et les échanges de vues ont donc été extrêmement enrichissants. La valeur de ces échanges tient en partie au fait que des points de vue divers, des idées nouvelles et des propositions importantes, y compris la possibilité de définir de nouvelles obligations juridiquement contraignantes, ont été mis en avant, même s'ils n'ont pas forcément fait l'unanimité parmi les États. Les différents points de vue exprimés sont reflétés dans le résumé des discussions et des formulations spécifiques proposées au titre du point de l'ordre du jour intitulé « Règles, normes et principes », qui a été établi par la présidence et joint au présent rapport. Ces éléments devraient être examinés plus avant lors de futurs processus organisés sous les auspices des Nations Unies, notamment dans le cadre des travaux du Groupe de travail à composition non limitée créé en application de la résolution 75/240 de l'Assemblée générale.

Annexe II*

Résumé de la présidence

A. Contexte

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

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

3. Le présent résumé est publié sous la responsabilité de la présidence et illustre sa vision des principaux points examinés lors des réunions du Groupe de travail à composition non limitée. Il se peut qu'il ne rende pas compte de toutes les contributions des délégations, et il ne doit pas être considéré comme l'expression de l'opinion consensuelle des États sur les points particuliers qui y sont abordés. Le recueil complet des déclarations et propositions soumises par les États pour distribution est disponible à l'adresse suivante : https://www.un.org/disarmament/open-ended-working-group.

B. Aperçu des débats

4. Les travaux menés par le Groupe de travail ont permis à tous les États d'exprimer leurs vues, leurs préoccupations et leurs aspirations de façon démocratique, transparente et inclusive. Bien que le Groupe se soit efforcé de recenser les domaines de convergence et de consensus, ses débats ont également illustré la diversité des perspectives, des idées et des propositions formulées par les États Membres et pourraient servir de point de départ utile à ses futurs travaux visant à parvenir à une vision commune de l'utilisation des TIC par les États dans le contexte de la sécurité internationale.

5. Tout au long de leurs délibérations au sein du Groupe de travail, les États ont souligné les liens et les synergies entre chacun des éléments du mandat du Groupe : les mesures prises par les États et les rapports entre ceux-ci sont régis par le droit

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

international, et les normes facultatives et non contraignantes fournissent des orientations supplémentaires sur ce qui constitue un comportement responsable de la part des États. Ces deux éléments illustrent les attentes en matière de comportement concernant les utilisations des TIC par les États dans le contexte de la sécurité internationale. De cette manière, ils contribuent également au renforcement de la confiance en accroissant la transparence et la coopération entre les États et en réduisant le risque de conflit. Le renforcement des capacités permet à son tour à tous les États de contribuer à l'accroissement de la stabilité et de la sécurité à l'échelle mondiale. Ensemble, ces éléments constituent un cadre global de mesures de coopération permettant de faire face aux risques qui se posent ou pourraient se poser dans le domaine des technologies numériques. Un dialogue institutionnel régulier permettra d'élaborer davantage ce cadre et de le rendre opérationnel en faisant progresser une vision commune, en échangeant les enseignements tirés et les bonnes pratiques en matière de mise en œuvre, en renforçant la confiance et en augmentant les capacités des États.

Menaces existantes et potentielles

6. Dans le cadre des débats du Groupe de travail, les États ont décrit des menaces existantes et potentielles très diverses, mettant en évidence le fait qu'ils pouvaient percevoir de différentes manières les menaces liées à l'environnement numérique. Le format inclusif du Groupe de travail a offert aux États la possibilité d'approfondir leur compréhension de la façon dont les autres percevaient les actions et les comportements dans l'environnement numérique, et d'entendre ce que les autres considéraient comme les menaces et les risques les plus importants.

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

8. Les États ont souligné que les mesures visant à promouvoir un comportement responsable des États devaient rester neutres sur le plan technologique, en faisant valoir que c'était l'utilisation abusive des technologies, et non les technologies elles-mêmes, qui était préoccupante. Ils ont reconnu que, même si les progrès technologiques et les nouvelles applications pouvaient offrir des possibilités de développement, ils pouvaient également étendre les surfaces d'attaque, amplifier les

vulnérabilités de l'environnement numérique ou être exploités aux fins d'activités malveillantes nouvelles. Des tendances et des développements technologiques particuliers ont été mis en évidence à cet égard, notamment les progrès de l'apprentissage automatique et de l'informatique quantique ; l'ubiquité des appareils connectés (« Internet des objets ») ; les nouvelles façons de stocker les données et d'y accéder au moyen de dispositifs d'enregistrement électronique partagés et de l'informatique en nuage ; et l'expansion des mégadonnées et des données personnelles numérisées.

Droit international

9. Guidés par le mandat du Groupe de travail, et dans le but de maintenir la paix et de la stabilité, de promouvoir un environnement numérique ouvert, sûr, stable, accessible et pacifique et de favoriser une compréhension commune, les États ont échangé leurs vues sur la manière dont le droit international s'appliquait à la dimension sécurité internationale des TIC.

10. Dans le cadre des débats du Groupe de travail, les États ont rappelé que le droit international et, en particulier, la Charte des Nations Unies, dans son intégralité, étaient applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement numérique ouvert, sûr, stable, accessible et pacifique. À cet égard, ils ont souligné qu'il fallait veiller à ce que chacun s'abstienne de prendre des mesures qui seraient contraires au droit international et à la Charte, entraveraient le plein développement économique et social des pays concernés et nuiraient au bien-être de leurs habitants. Ils ont dans le même temps souligné qu'il fallait mieux comprendre comment le droit international s'appliquait à l'utilisation des TIC par les États.

11. Parmi les principes spécifiques du droit international qui ont été réaffirmés figurent notamment la souveraineté des États ; l'égalité souveraine ; le règlement des différends internationaux par des moyens pacifiques, de telle manière que la paix et la sécurité internationales ainsi que la justice ne soient pas mises en danger ; le non-recours, dans les relations internationales, à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies ; le respect des droits humains et des libertés fondamentales ; la non-intervention dans les affaires intérieures d'autres États.

12. Il a été rappelé que le droit international était le fondement de la stabilité et de la prévisibilité des relations entre les États. En particulier, le droit international humanitaire réduisait les risques et les dommages qui pourraient être causés aux civils et aux biens de caractère civil ainsi qu'aux combattants dans le contexte d'un conflit armé. Dans le même temps, les États ont souligné que le droit international humanitaire n'encourageait pas la militarisation et ne légitimait pas non plus le recours au conflit dans quelque domaine que ce soit.

13. Il a également été noté qu'en vertu du droit international coutumier, la responsabilité des États en ce qui concernait les faits internationalement illicites s'étendait à leur utilisation des TIC.

14. Il a été rappelé que les États ne devaient pas faire appel à des intermédiaires pour commettre des faits internationalement illicites à l'aide des technologies numériques et devaient veiller à ce que des acteurs non étatiques agissant sur les instructions ou sous le contrôle d'un État n'utilisent pas leur territoire pour commettre de tels actes. La responsabilité des États a également été relevée en ce qui concernait les entités détenues ou contrôlées par l'État.

15. Les États ont rappelé que le signe qu'une activité numérique avait été lancée depuis le territoire ou les infrastructures numériques d'un État ou y trouvait son origine pouvait être insuffisant à lui seul pour imputer l'activité en question à cet État et que les accusations concernant l'organisation et l'exécution d'actes illicites portées contre des États devaient être étayées. Certains ont souligné qu'il importait de disposer de preuves authentiques, fiables et adéquates dans ce contexte.

16. Certains États ont estimé que le droit international en vigueur, complété par les normes facultatives et non contraignantes qui reflétaient le consensus entre les États, était actuellement suffisant pour traiter la question de l'utilisation des TIC par les États. Il a également été proposé de s'attacher à s'entendre sur la manière dont le cadre normatif déjà convenu s'appliquait en formulant d'autres orientations, et dont il pouvait être rendu opérationnel grâce à une meilleure application par tous les États. Dans le même temps, d'autres États ont estimé qu'en raison de l'évolution rapide du contexte de la menace et de la gravité du risque, un cadre juridiquement contraignant convenu au niveau international était nécessaire. Il a également été suggéré qu'un tel cadre contraignant pourrait conduire à une mise en œuvre plus efficace des engagements au niveau mondial et à l'établissement d'une base plus solide pour tenir les acteurs responsables de leurs actes. Les États ont souligné que tout cadre juridique international visant à traiter les questions relatives aux utilisations des TIC qui pourraient avoir une incidence sur la paix et la sécurité internationales devrait tenir compte des préoccupations et des intérêts de tous les États, reposer sur un consensus et être élaboré sous les auspices des Nations Unies, avec la participation active de tous les États, dans des conditions d'égalité.

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

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

19. Toujours en ce qui concerne les voies à suivre, les États ont avancé qu'une première étape clé pour clarifier et développer davantage les interprétations communes pourrait résulter d'échanges accrus et de discussions approfondies sur la manière dont le droit international s'appliquait à l'utilisation des TIC par les États. Il a été noté que ces échanges pourraient constituer en eux-mêmes une importante mesure de confiance. Certains États ont en outre proposé plusieurs moyens d'échanger à titre volontaire leurs vues nationales sur la façon dont s'appliquait le

droit international, notamment en utilisant le rapport annuel du Secrétaire général sur les progrès de l'informatique et des télécommunications et la sécurité internationale[9] et le portail des politiques de cybersécurité de l'Institut des Nations Unies pour la recherche sur le désarmement, ou en présentant une enquête sur les pratiques nationales en matière d'application du droit international. Les progrès réalisés quant aux accords régionaux et autres accords pour ce qui était d'échanger des points de vue et de parvenir à une compréhension commune de la manière dont le droit international s'appliquait ont également été soulignés.

20. S'agissant du maintien de la paix et de la prévention des conflits, les États ont affirmé qu'il importait de régler les différends par des moyens pacifiques et de s'abstenir de recourir à la menace ou à l'emploi de la force. Dans ce contexte, les États ont évoqué les organes, mécanismes et instruments existants pour la prévention et le règlement pacifique des différends. Certains ont suggéré que la promotion d'une approche et d'une compréhension communes et universellement acceptées de la source des incidents liés aux TIC au niveau technique sous les auspices des Nations Unies, grâce à la mise en commun de bonnes pratiques, en gardant à l'esprit le respect du principe de la souveraineté des États, pourrait permettre une meilleure application du principe de responsabilité et une transparence accrue, et contribuer à encourager les recours en justice lorsque des personnes étaient lésées par des actes de malveillance.

Normes, règles et principes relatifs au comportement responsable des États

21. Dans le cadre des débats du Groupe de travail, les États ont rappelé que les normes facultatives et non contraignantes de comportement responsable des États ne modifiaient pas le droit international ni les buts et principes des Nations Unies, notamment le maintien de la paix et de la sécurité internationales et la promotion des droits humains, et ne sauraient s'y substituer, mais qu'elles devaient plutôt être vues comme s'inscrivant dans le prolongement de ceux-ci. Ils ont également rappelé la résolution 2131 (XX) de l'Assemblée générale, en date du 21 décembre 1965, intitulée « Déclaration sur l'inadmissibilité de l'intervention dans les affaires intérieures des États et sur la protection de leur indépendance et de leur souveraineté ».

22. Les États ont rappelé que, dans sa résolution 73/27, l'Assemblée générale, tout en présentant un ensemble de 13 normes, règles et principes favorisant un comportement responsable des États, avait notamment accueilli favorablement les 11 normes facultatives et non contraignantes « énoncées et adoptées par consensus par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale dans ses rapports de 2013 et de 2015 et recommandées dans la résolution 71/28 »[10].

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

[9] A/RES/75/32.

[10] A/RES/73/27, par. 1.

24. Les États ont convenu que les normes pouvaient aider à prévenir les conflits dans la sphère numérique et contribuer à l'utilisation pacifique et pleinement utile des TIC en vue d'accroître le développement social et économique mondial. Ils ont souligné que l'application des normes ne devrait pas entraîner de restrictions indues en termes de coopération internationale et de transfert de technologie, ni entraver l'innovation à des fins pacifiques et le développement économique des États dans un environnement juste et non discriminatoire. Ils ont également mis l'accent sur les liens qui existaient entre les normes, le renforcement de la confiance et le renforcement des capacités et ont insisté sur la nécessité de tenir compte des questions de genre dans la mise en œuvre des normes.

25. Lors des discussions, il a été proposé d'affiner les normes existantes. Les États ont redit qu'il importait également de protéger toutes les infrastructures critiques qui étayaient les services essentiels destinés au public, notamment les installations médicales et les établissements de soins de santé. Ils ont également appelé l'attention sur le fait qu'il importait de coopérer pour protéger les infrastructures critiques qui fournissaient des services par-delà les frontières ou les juridictions, compte tenu des répercussions que tout dommage causé à ces infrastructures pourrait entraîner, et d'assurer la disponibilité générale et l'intégrité d'Internet. Ils ont rappelé la résolution 64/211 de l'Assemblée générale, intitulée « Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infostructures essentielles »[11]. Ils ont en outre proposé de mieux assurer l'intégrité de la chaîne d'approvisionnement en produits et services informatiques, en faisant part de leur préoccupation quant aux fonctionnalités cachées malveillantes des produits numériques, ainsi que le respect du principe de responsabilité s'agissant d'aviser les utilisateurs lorsque des vulnérabilités majeures étaient identifiées. Ils se sont également dits préoccupés par l'accumulation des vulnérabilités. Certains États ont proposé d'élaborer des règles et des normes internationales objectives en matière de sécurité de la chaîne d'approvisionnement.

26. Dans le prolongement du paragraphe ci-dessus, des propositions écrites formulées par les États dans le cadre des travaux du Groupe de travail au sujet de l'enrichissement des normes existantes, des orientations quant à leur mise en œuvre et de l'élaboration de nouvelles normes sont jointes en annexe.

27. Certains États ont également pris note du projet de code de conduite international pour la sécurité de l'information présenté en 2015[12].

28. Certains États ont reconnu la nécessité d'encourager et de soutenir d'autres initiatives régionales ainsi que des partenariats avec d'autres parties prenantes telles que le secteur privé et la communauté technique pour la mise en œuvre des normes. Ces partenariats pourraient être établis, par exemple, pour garantir des efforts durables de renforcement des capacités afin de remédier aux différences de capacités de mise en œuvre. À cet égard, les États ont rappelé le paragraphe 1.13 de la résolution 73/27 de l'Assemblée générale, qui dispose notamment que les États devraient inciter le secteur privé et la société civile à s'associer au renforcement de la sécurité numérique et à l'utilisation des technologies numériques, y compris pour ce qui est de la sécurité de la chaîne d'approvisionnement en produits et services numériques. Ils ont noté qu'il importait de prendre les mesures de sensibilisation et de coopération nécessaires pour que les différentes parties prenantes, y compris les secteurs public et privé et la société civile, assument leurs responsabilités quant à l'utilisation des TIC.

---

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

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

Mesures de confiance

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

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

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

32. Les États ont également appelé l'attention sur les rôles et responsabilités d'autres acteurs, y compris la société civile, le secteur privé, les universités et la communauté technique, s'agissant de contribuer à instaurer la confiance dans

l'utilisation des TIC aux niveaux national, régional et mondial. Ils ont souligné la diversité des initiatives multipartites qui, grâce à l'élaboration de principes et d'engagements, avaient permis d'établir de nouveaux réseaux d'échange, de collaboration et de coopération. Dans le même ordre d'idées, les initiatives sectorielles ou spécifiques à un domaine avaient fait la preuve de la prise de conscience croissante des rôles et responsabilités d'autres acteurs et des contributions uniques qu'ils pouvaient apporter à la sécurité des technologies de l'information et des communications au moyen d'engagements pris volontairement, ainsi que de normes et de codes professionnels.

Renforcement des capacités

33. Dans leurs débats dans le cadre du Groupe de travail, les États ont insisté sur la fonction importante que le renforcement des capacités peut remplir dans la mesure où il donne à tous les États les moyens de participer pleinement aux discussions menées à l'échelle internationale sur le cadre de comportement responsable des États, tout en contribuant aux engagements communs tels que le Programme de développement durable à l'horizon 2030[13]. À cet égard, les États ont fait valoir qu'il importe d'allouer des ressources financières et humaines suffisantes aux programmes de renforcement des capacités.

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

35. L'Organisation des Nations Unies a un rôle essentiel à jouer pour ce qui est d'aider les États à faire mieux connaître le renforcement des capacités et en tirant parti de sa puissance de rassemblement pour promouvoir une meilleure coordination des divers intervenants actifs dans le domaine du renforcement des capacités. Les États ont avancé que les instances existantes au sein du système des Nations Unies, ses institutions spécialisées et la communauté internationale au sens large pourraient être utilisées pour renforcer la coordination déjà établie. Ces instances pourraient être utilisées pour partager les points de vue nationaux sur les besoins en matière de renforcement des capacités, encourager le partage des enseignements tirés et des expériences acquises, tant par les bénéficiaires que par les fournisseurs de l'aide, et faciliter l'accès aux informations sur les programmes de renforcement des capacités et d'assistance technique. Elles pourraient également promouvoir la mobilisation des ressources ou aider à jumeler les ressources disponibles avec les demandes d'appui au renforcement des capacités et d'assistance technique. Il a été suggéré que l'élaboration d'un programme mondial de renforcement des cybercapacités sous les auspices des Nations Unies pourrait contribuer à assurer une plus grande cohérence des efforts de renforcement des capacités et que des enquêtes d'auto-évaluation effectuées à titre volontaire pourraient aider les États à identifier et à hiérarchiser leurs besoins en matière de renforcement des capacités ou leur capacité de fournir un appui.

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

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

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

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

Dialogue institutionnel régulier

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

40. Les États ont exprimé diverses opinions quant aux objectifs qui devraient constituer la priorité d'un futur dialogue institutionnel régulier et quant à la structure de dialogue régulier qui pourrait le mieux concourir à la réalisation de ces objectifs. Certains États ont émis le souhait qu'un dialogue régulier ait pour objectif prioritaire la concrétisation des engagements et recommandations existants, notamment l'élaboration d'orientations pour en appuyer et en suivre la mise en œuvre ; la

coordination et le renforcement de l'efficacité du renforcement des capacités ; et l'inventaire et l'échange de bonnes pratiques. D'autres États ont exprimé le souhait qu'un dialogue régulier privilégie l'étoffement des engagements existants et la définition de nouveaux engagements, y compris la négociation d'un instrument juridiquement contraignant et des structures institutionnelles qui l'étayent.

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

42. Les États ont pris note de la création, par la résolution 75/240 en date du 31 décembre 2020, d'un nouveau groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), qui commencera ses activités dès la conclusion des travaux du groupe de travail à composition non limitée créé par la résolution 73/27 et examinera les résultats de ces travaux.

43. Les États ont également exprimé le souhait que la communauté internationale revienne à terme à un processus unique fondé sur le consensus, sous les auspices des Nations Unies. À cet égard, ils ont noté que les différentes formules proposées pour le dialogue ne s'excluent pas nécessairement les unes les autres. Il a été suggéré que différentes formules pourraient se compléter ou être regroupées afin de tirer pleinement parti des caractéristiques uniques de chacune et de réduire le double emploi.

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

45. Tout en reconnaissant le rôle et la responsabilité uniques qui sont les leurs en matière de sécurité nationale et internationale, les États ont souligné la contribution importante qu'un comportement responsable des autres acteurs apporte à un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies numériques. À cet égard, il a été noté que le renforcement de la coopération et des partenariats multipartites pourrait favoriser la création d'un environnement numérique plus résilient et plus sûr.

Annexe au résumé du Président

Formulations spécifiques proposées au titre du point de l'ordre du jour « Règles, normes et principes » à partir des soumissions écrites reçues des délégations.

Compte tenu que, dans leurs contributions écrites, de nombreuses délégations ont fait référence à des normes existantes, le texte ci-dessous ne reflète que des propositions d'éléments supplémentaires.

Arménie

• Les États s'abstiendront de toute action susceptible d'entraîner une tentative de perturber l'intégrité des infrastructures critiques et les activités gouvernementales, et offriront, par des voies sécurisées, des éclaircissements en temps utile afin de prévenir toute autre escalade éventuelle.

Australie, Estonie, États-Unis d'Amérique, Japon, Kazakhstan et République tchèque

Texte fournissant des orientations sur la mise en œuvre des normes de 2015 – alinéas f) et g) du par. 13

• En fournissant des orientations pour la mise en œuvre de ces normes, les États devraient noter que les secteurs cités comme des éléments de l'infrastructure critique ne sont pas censés constituer une liste exhaustive et que leur désignation à ce titre n'a aucune incidence sur le classement (ou le non-classement) national de tout autre secteur, pas plus qu'elle n'autorise implicitement une activité malveillante contre une catégorie qui n'est pas nommée.

• Le Groupe de travail a établi son rapport dans le contexte de la pandémie de COVID-19. Dans ces circonstances, le Groupe de travail a souligné que tous les États considéraient les services médicaux et les installations médicales comme des infrastructures essentielles aux termes des alinéas f) et g).

Bélarus

• Les États devraient réaffirmer leurs engagements à l'égard du principe consistant à s'abstenir de militariser les TIC existantes et de créer de nouvelles TIC conçues expressément pour nuire aux ressources, aux infrastructures et aux installations essentielles d'autres États en matière d'information.

Canada

Texte d'orientation sur les normes qu'il est proposé d'ajouter au paragraphe 41

Alors que les normes de 2015 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale précisent les actions que les États devraient ou ne devraient pas prendre, les États ont souligné qu'il faut des orientations sur la manière de traduire les normes sur le plan opérationnel et proposé les éléments suivants. Dans l'esprit des membres du Groupe de travail, les normes et les orientations sont sans préjudice des droits et obligations existants des États en vertu du droit international et ne les modifient ni ne les diminuent en aucune façon.

a. Conformément aux buts des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, les États coopèrent 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 ou susceptibles de compromettre la paix et la sécurité internationales (2015, alinéa a) du par. 13).

i. Cette norme est de nature générale. La mise en œuvre de l'ensemble des normes, ainsi que les orientations spécifiques fournies ci-dessous, contribueront à concrétiser davantage cette norme. Les États devraient adopter une démarche concertée pour travailler les uns avec les autres ainsi qu'avec les acteurs non gouvernementaux, y compris l'industrie, les universités et la société civile.

ii. Pour ce faire, les États devraient, le cas échéant et dans la mesure du possible :

– adopter et mettre en œuvre des stratégies nationales intégrées en matière de cybersécurité. Dans la mesure du possible, ils devraient préconiser la coopération internationale en la matière ;

– mettre en place et maintenir des fonctions d'intervention en cas d'incident informatique, par exemple des équipes d'intervention rapide dans le domaine informatique qui soient capables d'assumer un rôle de coordination, de partager les bonnes pratiques et de coopérer en réponse aux incidents informatiques ;

– publier des déclarations indiquant qu'ils agiront conformément au cadre de comportement responsable des États dans le cyberespace, tel qu'il est défini dans le rapport de 2015 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale ;

– participer aux initiatives régionales et bilatérales qui visent à élaborer et à mettre en œuvre des mesures de confiance.

iii. Les États Membres devraient être encouragés à compiler et à réorganiser les informations qu'ils présentent sur leur mise en œuvre des normes convenues.

b. En cas d'incident informatique, 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'incident (2015, alinéa b) du par. 13).

i. Les États pourraient se doter des structures, politiques, processus et mécanismes de coordination nationaux nécessaires pour faciliter l'examen attentif des incidents informatiques graves et pour déterminer les mesures qui s'imposent.

ii. Une fois ces structures et processus en place, les États pourraient élaborer des modèles d'évaluation des incidents informatiques ou des grilles d'évaluation pour permettre de décrire les incidents et d'en évaluer la gravité.

iii. L'harmonisation de ces grilles par les organisations régionales et la transparence à leur sujet pourraient garantir que les États considèrent les incidents informatiques de manière cohérente et améliorer la communication entre les États. Dans la mesure du possible, les grilles devraient être conformes aux pratiques existantes et ne pas faire double emploi.

iv. Lors de l'examen de toutes les informations pertinentes dans le cas d'un incident informatique, les États devraient mener des recherches sur les incidences genrées possibles et travailler de manière inclusive avec toutes les parties prenantes pour comprendre le contexte plus large de l'incident, y compris son impact sur la jouissance des droits humains des personnes LGBT et des femmes.

v. Les États devraient tenir compte de l'effet des incidents informatiques sur les droits humains, notamment les droits à la liberté d'expression, d'association et de réunion pacifique, le droit de chaque personne de ne pas faire l'objet d'immixtions arbitraires ou illégales dans sa vie privée, et les droits des personnes handicapées.

vi. Les États devraient reconnaître que les interventions en cas d'atteinte à la sécurité nécessitent souvent la mise à contribution de divers acteurs (ne se limitant pas aux équipes nationales d'intervention rapide dans le domaine informatique ou d'intervention en cas d'atteinte à la sécurité informatique), et améliorer la collaboration par la formation et le renforcement des capacités de tous les groupes de parties prenantes. Les États devraient encourager la formation à la sécurité numérique et d'autres mesures de renforcement des capacités et d'assistance par les parties prenantes, y compris la société civile, ayant pour objectif de prévenir les atteintes à la sécurité, en particulier pour les groupes vulnérables et les autres utilisateurs à risque.

c. Les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications (2015, alinéa c) du par. 13).

i. En ce qui concerne la mise en œuvre de cette norme :

– Si un État constate une cyberactivité malveillante émanant du territoire ou de la cyberinfrastructure d'un autre État, la première étape pourrait consister à en aviser cet État. Les équipes d'intervention rapide dans le domaine informatique sont essentielles pour pouvoir repérer ce type d'activité.

– Étant donné que les incidents informatiques peuvent émaner d'États tiers ou les impliquer, il est entendu que le fait d'aviser un État n'implique pas la responsabilité de cet État dans l'incident.

– L'État qui a reçu un tel avis doit accuser réception de la demande par l'intermédiaire du point de contact national concerné.

– Lorsqu'un État sait que son territoire ou sa cyberinfrastructure sont utilisés pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications et que ces faits sont susceptibles d'entraîner des conséquences négatives graves dans un autre État, il doit s'efforcer de prendre des mesures raisonnables, concrètes et réalisables sur son territoire et dans la limite de ses capacités, conformément aux obligations que lui impose le droit interne et international, pour faire cesser le fait internationalement illicite ou en atténuer les conséquences.

– Un État peut prendre conscience d'un tel acte par suite d'un avis reçu d'un État touché. Cette notification doit être faite de bonne foi et doit être accompagnée d'informations justificatives. Parmi ces informations complémentaires peuvent figurer le partage d'éventuels indicateurs de compromission, tels que l'adresse de protocole Internet (adresse IP) et les ordinateurs utilisés pour les actes malveillants et les informations relatives aux logiciels malveillants utilisés.

– Les États devraient être encouragés à veiller à ce que les acteurs non étatiques, y compris ceux du secteur privé, soient empêchés de mener des activités informatiques malveillantes à leurs propres fins ou à celles d'acteurs étatiques ou non étatiques, au détriment de tiers, y compris ceux situés sur le territoire d'un autre État. Cet objectif pourrait être atteint grâce à une collaboration avec le secteur privé visant à définir les actions acceptables au moyen d'une approche fondée sur les risques et à élaborer des outils concrets : procédures de certification, guides des meilleures pratiques, mécanismes d'intervention et, le cas échéant, réglementations nationales.

– Cette norme ne doit pas être interprétée comme exigeant d'un État qu'il surveille de manière proactive toutes les technologies numériques présentes sur son territoire, ou qu'il prenne d'autres mesures préventives.

ii. Un État qui a connaissance d'activités informatiques préjudiciables émanant de son territoire mais qui n'a pas la capacité de réagir peut choisir de demander l'aide d'autres États, notamment par le biais de formulaires standard de demande d'assistance.

– En pareil cas, un État peut demander l'assistance d'autres États ou d'une entité privée. Le cas échéant, l'aide doit être fournie dans le respect du droit national, et du droit international des droits de l'homme.

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 des technologies de l'information et des communications et appliquer d'autres mesures collectives afin de parer à ces risques ; à cet égard, les États peuvent être amenés à déterminer si de nouvelles mesures doivent être élaborées (2015, alinéa d) du par. 13).

i. Dans l'application de cette norme, les États devraient :

– envisager, le cas échéant, de soutenir les travaux de la Commission pour la prévention du crime et la justice pénale, notamment en prorogeant le mandat du groupe intergouvernemental d'experts à composition non limitée, et en appuyant les efforts qu'il déploie pour étudier, de manière globale, le problème de la cybercriminalité ;

– soutenir l'action menée par l'Office des Nations Unies contre la drogue et le crime pour continuer à fournir aux États Membres, sur demande et en fonction de leurs besoins nationaux, une assistance technique et des services de renforcement durable des capacités pour les aider à faire face à la cybercriminalité, par l'intermédiaire du Programme mondial contre la cybercriminalité et, entre autres, de ses bureaux régionaux, en ce qui concerne la prévention, la détection, les enquêtes et les poursuites visant la cybercriminalité sous toutes ses formes, sachant que la coopération avec les États Membres, les organisations internationales et régionales compétentes, le secteur privé, la société civile et les autres parties prenantes peut faciliter cette activité ;

– mettre en œuvre les mesures existantes d'une manière qui soit conforme à leurs obligations et envisager de prendre de nouvelles mesures, comme l'adoption d'une législation nationale pour lutter contre la cybercriminalité, d'une manière qui soit conforme aux obligations des États en matière de droits humains et qui offre des garanties judiciaires.

e. Les États, lorsqu'ils veillent à une utilisation sûre des technologies de l'information et des communications, 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 de l'homme 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 de l'homme, y compris le droit à la liberté d'expression (2015, alinéa e) du par. 13).

i. Les États devraient :

– s'acquitter des obligations qui leur incombent en vertu du droit national et international, lorsqu'ils envisagent, élaborent ou appliquent des politiques ou des législations nationales en matière de cybersécurité ou lorsqu'ils conçoivent et mettent en place des initiatives ou des structures liées à la cybersécurité, y compris des mesures visant à garantir la protection de tous les droits humains ;

– ce faisant, prendre en compte les points de vue de toutes les parties intéressées et touchées dès les premières étapes de l'élaboration et de la mise en œuvre des politiques de cybersécurité, afin de garantir une prise en compte globale des implications des mesures de cybersécurité ;

– ne pas perdre de vue que la participation de la société civile est particulièrement importante, étant donné son rôle d'acteur clé dans la promotion du respect par les États de leurs obligations et engagements en matière de droits humains ;

– prendre en considération le fait que les individus ont les mêmes droits en ligne que hors ligne, et devraient garder à l'esprit les menaces spécifiques que les femmes et les individus appartenant à des groupes minoritaires et vulnérables peuvent subir en ce qui a trait à leurs droits humains ;

– réaliser des audits de genre des politiques nationales ou régionales de cybersécurité afin de recenser les domaines à améliorer ;

– envisager d'intégrer des mesures visant à remédier aux implications des technologies de l'information et des communications pour les droits humains dans leurs plans d'action nationaux relatifs aux entreprises et aux droits humains.

f. Un État ne devrait pas mener ou soutenir sciemment une activité informatique qui est contraire aux obligations qu'il a contractées en vertu du droit international et qui endommage intentionnellement une infrastructure essentielle ou qui compromet l'utilisation et le fonctionnement d'une infrastructure essentielle pour fournir des services au public (2015, alinéa f) du par. 13).

i. Chaque État détermine les infrastructures ou les secteurs qu'il juge critiques, en fonction des priorités nationales et des méthodes de catégorisation des infrastructures critiques. Parmi les exemples de secteurs d'infrastructures critiques qui fournissent des services publics essentiels, on peut citer l'énergie, l'eau, l'assainissement, la santé, l'éducation, les finances, les transports, les télécommunications et les organisations qui interviennent en cas de crise. Les infrastructures critiques pourraient également comprendre les infrastructures techniques essentielles aux élections, référendums ou plébiscites et les infrastructures techniques essentielles à la disponibilité générale ou à l'intégrité de l'Internet. Le fait que ces infrastructures

soient citées en guise d'exemples n'empêche pas les États de qualifier de critiques d'autres éléments d'infrastructure, pas plus qu'il n'autorise implicitement une activité malveillante contre une catégorie qui n'est pas nommée.

ii. Les États doivent tenir compte des effets potentiellement dommageables de leurs activités informatiques sur les infrastructures techniques essentielles à la disponibilité générale ou à l'intégrité de l'Internet.

g. Les États devraient prendre les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux technologies de l'information et des communications en tenant compte de la résolution 58/199 de l'Assemblée générale sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information et d'autres résolutions pertinentes (2015, alinéa g) du par. 13).

i. Afin de contribuer à une culture mondiale de la cybersécurité, les États devraient envisager, le cas échéant, de partager des informations sur les meilleures pratiques en matière de protection des infrastructures critiques, y compris tous les éléments recensés dans la présente résolution et sur :

– les exigences de base en matière de sécurité ;

– les procédures de notification des incidents ;

– les outils et méthodologies de traitement des incidents ;

– la résilience face aux situations d'urgence ;

– les enseignements tirés d'incidents précédents.

ii. Les mesures de renforcement des capacités et les autres mesures visant à instaurer une culture mondiale de la cybersécurité devraient être élaborées de manière inclusive et s'efforcer de tenir compte de la dimension de genre des questions de cybersécurité.

iii. Compte tenu de la nature variée et décentralisée de la propriété des infrastructures critiques, les États devraient, le cas échéant, et en consultation avec les acteurs intéressés, promouvoir des normes minimales pour la sécurité des infrastructures critiques et favoriser la coopération avec le secteur privé, les universités et la communauté technique, s'agissant de protéger les infrastructures critiques.

iv. Les États devraient, le cas échéant, participer à des initiatives volontaires d'évaluation des risques et de planification de la continuité des opérations (résilience, reprise et interventions d'urgence) faisant intervenir d'autres acteurs et visant à renforcer, face aux menaces existantes et émergentes, la sécurité et la résilience des infrastructures critiques qui fournissent des services au niveau régional ou international.

v. Il faudrait prendre des mesures visant à protéger les infrastructures d'information critiques en tenant dûment compte des lois nationales applicables en matière de protection de la vie privée et des autres législations pertinentes.

vi. En fournissant des orientations pour la mise en œuvre des normes f) et g), les États devraient noter que les secteurs cités en tant qu'éléments de l'infrastructure critique ne sont pas censés constituer une liste exhaustive et que leur désignation à ce titre n'a aucune incidence sur le classement (ou le non-classement) national de tout

autre secteur, pas plus qu'elle n'autorise implicitement une activité malveillante contre une catégorie qui n'est pas nommée.

vii. Le Groupe de travail a souligné que tous les États considéraient les services médicaux et les installations et infrastructures médicales comme des infrastructures essentielles aux termes des normes f) et g). Il a paru d'autant plus essentiel de préconiser la protection des infrastructures de santé que le Groupe a établi son rapport dans le contexte de la pandémie de COVID-19.

> 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 informatiques malveillantes dirigées contre une infrastructure essentielle d'un autre État et exercées depuis leur territoire, en tenant dûment compte de la souveraineté (2015, alinéa h) du par. 13).

i. La mise en œuvre de cette norme implique l'examen des demandes d'assistance appropriées et la prise en compte de la nature de l'assistance qui peut être offerte en temps opportun. L'État qui reçoit une demande d'assistance appropriée à la suite d'un incident informatique devrait envisager, lorsque cela semble possible, raisonnable et approprié :

- d'accuser réception de la demande par l'intermédiaire du point de contact national concerné ;
- de déterminer, en temps utile, s'il a la capacité et les ressources nécessaires pour fournir l'assistance demandée. Il peut s'agir de repérer les connaissances spécialisées disponibles au pays parmi une série de parties prenantes ;
- dans sa réponse initiale, d'indiquer la nature, la portée et les conditions de l'assistance qui pourrait être fournie, y compris un calendrier pour sa prestation ;
- s'il est convenu de fournir une assistance, de fournir rapidement l'assistance prévue ;
- de veiller à ce que les demandes d'assistance, y compris les procédures et ressources pertinentes, telles que les cadres et les modèles, et les interventions respectent les obligations en matière de droits humains.

ii. La mise en œuvre de cette norme serait facilitée davantage par l'existence préalable de structures et de mécanismes nationaux, y compris un point de contact national et des modèles pour les demandes d'assistance et la confirmation de l'assistance convenue, et par un renforcement des capacités et une assistance technique ciblés. Les initiatives de coopération bilatérale et multilatérale, les organisations et les instances internationales et régionales peuvent contribuer à faciliter le développement de ces moyens.

Parmi les approches qui pourraient contribuer positivement à la mise en œuvre de cette norme, citons : une collaboration accrue entre les secteur public et privé et les organisations de la société civile, au niveau national et international, en particulier pour ce qui est de prendre des mesures préventives ; l'amélioration de la capacité des équipes d'intervention par une approche adaptée du développement de la cybercapacité ; et des formations spécialisées visant à renforcer les cybercapacités à tous les niveaux des États et de la société.

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 informatiques, et devraient s'attacher à prévenir la prolifération des techniques et des outils informatiques malveillants et l'utilisation de fonctionnalités cachées malveillantes (2015, alinéa i) du par. 13).

i. Pour appliquer cette norme, les États devraient :

– prendre des mesures, notamment par le biais des instances existantes, pour prévenir la prolifération des techniques et des outils informatiques malveillants. Ce faisant, les États devraient encourager les activités légitimes des communautés de recherche, des universités, de l'industrie, des services répressifs, des équipes d'intervention rapide dans le domaine informatique /équipes d'intervention en cas d'atteinte à la sécurité informatique et d'autres organismes de cyberprotection qui concourent à assurer la sécurité de leurs systèmes informatiques ;

– envisager l'échange d'informations sur les vulnérabilités liées aux TIC et/ou les fonctions cachées nuisibles dans les produits informatiques ;

– travailler à la mise en œuvre de contrôles de sécurité fondés sur la gestion des risques.

j. Les États devraient encourager le signalement responsable des failles informatiques et partager les informations sur les moyens permettant de les corriger, afin de limiter et éventuellement d'éliminer les risques pour les systèmes qui utilisent les technologies de l'information et des communications et pour les infrastructures qui en dépendent (2015, alinéa j) du par. 13).

i. Pour appliquer cette norme, les États devraient :

– mettre en place des structures nationales permettant de signaler et de traiter de manière responsable les vulnérabilités informatiques ;

– promouvoir les mécanismes de coordination appropriés entre les entités des secteurs public et privé.

ii. En outre, et afin d'éviter les malentendus ou les interprétations erronées, notamment ceux qui découlent de la non-divulgation d'informations sur les vulnérabilités informatiques potentiellement dangereuses, les États sont encouragés à partager, le cas échéant, dans la mesure la plus large possible, les informations techniques sur les incidents informatiques graves, en utilisant les mécanismes de coordination existants entre équipes d'intervention rapide dans le domaine informatique, ainsi que les mécanismes mis en place par les organisations régionales (tels que les réseaux de points de contact). Les États devraient veiller à ce que ces informations soient traitées de manière responsable et en coordination avec d'autres parties prenantes, le cas échéant.

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 (2015, alinéa k) du par. 13).

Chine

• Les États devraient s'engager à ne pas utiliser les technologies de l'information et des communications et les réseaux numériques pour mener des activités qui vont à l'encontre du maintien de la paix et de la sécurité internationales.

Souveraineté des États dans le cyberespace

• Les États devraient exercer leur compétence territoriale pour ce qui est de leur utilisation du numérique et de leurs infrastructures numériques.

• Les États ont le droit d'élaborer des politiques publiques conformes à leur législation pour gérer leurs propres affaires dans le domaine du numérique et protéger les intérêts légitimes de leurs citoyens dans le cyberespace.

• Les États devraient s'abstenir d'utiliser les technologies de l'information et des communications pour s'ingérer dans les affaires intérieures d'autres États et compromettre leur stabilité politique, économique et sociale.

• Les États doivent participer à la gestion et à la distribution des ressources Internet internationales sur un pied d'égalité.

Protection des infrastructures critiques

• Les États ont le droit et la responsabilité de protéger juridiquement leurs infrastructures numériques critiques contre les dommages causés par des menaces, des interférences, des attaques et des opérations de sabotage.

• Les États devraient s'engager à s'abstenir de lancer des cyberattaques contre les infrastructures critiques d'autres États.

• Les États ne devraient pas utiliser leurs avantages politiques et techniques pour porter atteinte à la sécurité et à l'intégrité des infrastructures critiques d'autres États.

• Les États devraient accroître les échanges sur les normes et les meilleures pratiques en matière de protection des infrastructures critiques et encourager les entreprises à y participer.

Sécurité des données

• Les États devraient envisager les questions relatives aux progrès techniques, au développement des entreprises et à la sauvegarde de la sécurité nationale et de l'intérêt public de manière équilibrée.

• Les États ont le droit et la responsabilité de garantir la sécurité des données et des informations personnelles importantes ayant une incidence sur leur sécurité nationale, leur sécurité publique, leur sécurité économique et leur stabilité sociale.

• Les États doivent s'abstenir de mener ou de soutenir des activités d'espionnage informatique ciblant d'autres États, comme la surveillance de masse ou le vol de données importantes et d'informations personnelles.

• Les États devraient accorder une attention égale au développement et à la sécurité, et faire pression pour que les données circulent de manière légale, ordonnée et libre. Les États devraient faciliter les échanges de bonnes pratiques et la coopération à cet égard.

Sécurité de la chaîne d'approvisionnement

• Les États ne devraient pas profiter de leur position dominante dans le domaine de l'informatique et des communications, y compris en matière de ressources, d'infrastructures critiques et de technologies de base, et de biens et de services numériques, pour porter atteinte au droit d'autres États de contrôler de manière autonome ces produits et services et leur sécurité.

• Les États devraient interdire aux fournisseurs de produits et services numériques d'installer des portes dérobées dans leurs produits pour obtenir illégalement des données d'utilisateurs ou contrôler et manipuler les dispositifs et systèmes de ceux-ci. Les États devraient également interdire aux fournisseurs de produits et services numériques de chercher à servir des intérêts illégitimes en profitant de la dépendance des utilisateurs à l'égard de leurs produits, ni forcer les utilisateurs à mettre à niveau leurs systèmes et dispositifs. Les États devraient demander aux fournisseurs de produits et services numériques de s'engager à ce que leurs partenaires de coopération et leurs utilisateurs soient avertis en temps utile en cas de détection de vulnérabilités graves dans leurs produits.

• Les États doivent s'engager à maintenir un environnement commercial équitable, juste et non discriminatoire. Ils ne devraient pas utiliser la sécurité nationale comme prétexte pour restreindre le développement et la coopération en matière d'informatique et de communications et limiter l'accès au marché des produits numériques et l'exportation de produits de haute technologie.

Lutte contre le terrorisme

• Les États devraient empêcher les organisations terroristes d'utiliser Internet pour créer des sites Web, des forums en ligne et des blogs aux fins de la conduite d'activités terroristes, notamment la fabrication, la publication, le stockage et la diffusion de documents audio et vidéo, la diffusion de discours et d'une idéologie terroristes violentes, la collecte de fonds, le recrutement et l'incitation à commettre des actes terroristes.

• Les États devraient échanger des renseignements et faire en sorte que leurs services de répression coopèrent pour lutter contre le terrorisme. Par exemple, dans les affaires de cyberterrorisme, lorsque d'autres États lui en font la demande, il convient qu'un État stocke et collecte des données et des preuves numériques pertinentes dans les meilleurs délais, facilite les enquêtes et se montre réactif.

• Les États devraient développer un partenariat de coopération avec les organisations internationales, les entreprises et les citoyens aux fins de la lutte contre le cyberterrorisme.

• Les États devraient demander aux fournisseurs d'accès à Internet de couper le canal de diffusion en ligne des contenus terroristes en fermant les sites et les comptes consacrés à la propagande et en supprimant les contenus terroristes et extrémistes violents.

Croatie, Finlande, France et Slovénie

- Les États devraient être encouragés à veiller à ce que les acteurs non étatiques, y compris ceux du secteur privé, soient empêchés de mener des activités informatiques malveillantes à leurs propres fins ou à celles d'acteurs étatiques ou non étatiques, au détriment de tiers, y compris ceux situés sur le territoire d'un autre État.

- Cet objectif pourrait être atteint grâce à une collaboration avec le secteur privé visant à définir les actions acceptables au moyen d'une approche fondée sur les risques et à élaborer des outils concrets : procédures de certification, guides des meilleures pratiques, mécanismes d'intervention et, le cas échéant, réglementations nationales.

Cuba

La situation actuelle nécessite que des réglementations spécifiques soient mises en place pour compléter le droit international en vue de réaliser les objectifs suivants, lesquels sont tous aussi importants les uns que les autres :

- Empêcher l'application de mesures unilatérales et de mesures visant certains États, compte tenu qu'elles entravent l'accès universel aux avantages offerts par les technologies de l'information et des communications.

- Atténuer les conséquences pernicieuses que peut avoir l'attribution des responsabilités en cas de cyberattaque.

- Prévenir la militarisation du cyberespace.

- Protéger plus efficacement les données privées des citoyens par la promotion de réglementations internationales.

- Compléter la législation relative au cyberterrorisme en vigueur en vue de faire face aux problèmes de cybersécurité, tels que les cyberattaques. Définir par consensus ce que l'on entend par cyberattaque.

- Faire appliquer avec une plus grande objectivité les principes du droit international dans ce domaine.

République tchèque

- Les États ne devraient pas mener ou soutenir sciemment une cyberactivité qui vise à porter atteinte à des services de santé ou à des installations médicales, et devraient prendre des mesures pour protéger les services de santé contre toute activité nocive[14].

- Les États devraient respecter les obligations existantes en vertu du droit international des droits de l'homme lors de l'examen, de l'élaboration et de l'application des politiques et de la législation nationales en matière de cybersécurité[15].

- Les États devraient prendre en compte les points de vue de toutes les parties intéressées et touchées dès les premières étapes de l'élaboration et de la mise en œuvre

[14] https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law.

[15] https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf.

des politiques de cybersécurité, afin de garantir une prise en compte globale des implications des mesures de cybersécurité[16].

Équateur

• Les orientations suivantes sont proposées pour la mise en œuvre de la norme figurant à l'alinéa b) du paragraphe 13 du rapport de 2015 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale[17] :

i) Les États pourraient se doter des structures, politiques, processus et mécanismes de coordination nationaux nécessaires pour faciliter l'examen attentif des incidents informatiques graves et pour déterminer les mesures qui s'imposent ;

ii) Les États pourraient ensuite élaborer des modèles d'évaluation des incidents informatiques ou des grilles d'évaluation pour permettre de décrire les incidents et d'en évaluer la gravité ;

iii) L'harmonisation de ces grilles par les organisations régionales et la transparence à leur sujet pourraient garantir que les États considèrent les incidents informatiques de manière cohérente et améliorer la communication entre les États ;

iv) Lors de l'examen de toutes les informations pertinentes dans le cas d'un incident informatique, les États devraient mener des recherches sur les incidences genrées possibles et travailler de manière inclusive avec toutes les parties prenantes pour comprendre le contexte plus large d'un incident, y compris son impact sur la jouissance des droits humains des femmes.

• Les orientations suivantes sont proposées pour la mise en œuvre de la norme figurant à l'alinéa c) du paragraphe 13[18] :

i) Si un État constate une cyberactivité malveillante émanant du territoire ou de la cyberinfrastructure d'un autre État, la première étape pourrait consister à en aviser cet État. Les équipes d'intervention rapide dans le domaine informatique sont essentielles pour pouvoir repérer ce type d'activité.

ii) Étant donné que les incidents informatiques peuvent émaner d'États tiers ou les impliquer, il est entendu que le fait d'aviser un État n'implique pas la responsabilité de cet État dans l'incident.

iii) L'État qui a reçu un tel avis doit accuser réception de la demande par l'intermédiaire du point de contact national concerné.

iv) Lorsqu'un État sait que son territoire ou sa cyberinfrastructure sont utilisés pour commettre des faits internationalement illicites et susceptibles d'entraîner des conséquences négatives graves dans un autre État, il doit s'efforcer de prendre des mesures raisonnables, concrètes et réalisables sur son territoire et dans la limite de ses capacités, conformément aux obligations que lui impose le droit interne et international, pour faire cesser le fait internationalement illicite ou en atténuer les conséquences.

---

[16] https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber- Security-07.02.pdf.

[17] En cas d'incident informatique, 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'incident.

[18] Les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications.

v) Cette norme ne doit pas être interprétée comme exigeant d'un État qu'il surveille de manière proactive toutes les technologies numériques présentes sur son territoire, ou qu'il prenne d'autres mesures préventives.

vi) Un État qui a connaissance d'activités informatiques préjudiciables émanant de son territoire mais qui n'a pas la capacité de réagir peut choisir de demander l'aide d'autres États, notamment par le biais de formulaires standard de demande d'assistance.

vii) En pareil cas, un État peut demander l'assistance d'autres États ou d'une entité privée, dans le respect du droit national. L'engagement des États à coopérer avec d'autres nations et à les aider en cas de crise est essentiel, l'accent devant être mis sur les effets différenciés que pourrait avoir un incident informatique sur une infrastructure spécifique dans un pays en développement.

- Le projet devrait également comprendre de nouvelles normes, dont la suivante :

« Les États ne devraient pas mener d'activités informatiques qui visent à perturber l'infrastructure technique essentielle aux processus politiques, tels que les élections, les référendums ou les plébiscites ».

Inde

- (à propos du paragraphe 39) Proposition d'une nouvelle norme (dans le contexte de la nécessité de convenir d'une règle concernant les questions essentielles de sécurité dans le cyberespace) sur les moyens les plus efficaces d'optimiser les technologies prometteuses tout en protégeant le public. Cette norme suppose que les États soutiennent fermement et unanimement l'adoption de normes en matière d'hygiène numérique de base et la vérification de leur mise en œuvre.

- Les États sont responsables de la protection des infrastructures d'information critiques. Lorsque les infrastructures d'information critiques d'une nation sont exposées à des menaces, l'intégrité des données de cette nation peut être compromise et son économie et développement économique, endommagés. Les États doivent envisager de protéger ces infrastructures au moyen de partenariats public-privé. Les États ne devraient pas mener d'activités informatiques qui visent à perturber les infrastructures d'information critiques. Les États ne devraient pas créer de fonctionnalités malveillantes dans leurs produits numériques. Les États devraient avertir les utilisateurs lorsque des vulnérabilités importantes sont détectées et en aviser les vendeurs afin qu'ils règlent le problème. Les États devraient collaborer dans le domaine des infrastructures d'information critiques, échanger des informations sur les menaces et partager les outils et techniques qui permettent d'atténuer ces dernières.

République islamique d'Iran

- Les États, dont la responsabilité première est de maintenir un environnement numérique sûr, sécurisé et fiable, devraient jouer un rôle plus important en ce qui concerne la gouvernance de l'environnement numérique, notamment pour ce qui est de l'élaboration de politiques et de la prise de décision au niveau mondial. Cela devrait être envisagé d'une manière qui renforce leur souveraineté et ne change pas leurs droits s'agissant des modèles de développement, de gouvernance et de législation qu'ils choisissent pour leur environnement numérique.

- Les États devraient s'abstenir de recourir à la menace ou à l'emploi de la force contre l'intégrité territoriale ou l'indépendance politique de tout État dans l'environnement numérique.

- Aucun État n'a le droit d'intervenir par des voies et moyens informatiques, directement ou indirectement et pour quelque raison que ce soit, dans les affaires intérieures ou extérieures d'autres États. Toutes les formes d'intervention et d'ingérence ou de tentative de menace à l'encontre des systèmes politiques, économiques, sociaux et culturels ainsi que des infrastructures critiques liées au cyberespace des États doivent être prévenues et sanctionnées (résolution 2131 de l'Assemblée générale datée du 21 décembre 1965).

- Les États ne doivent pas utiliser les progrès de l'informatique et des communications pour mettre en place des mesures coercitives (économiques, politiques ou de tout autre nature) contre d'autres États, notamment des mesures de blocage et de limitation (résolution 2131 de l'Assemblée générale datée du 21 décembre 1965).

- Les États devraient prendre des mesures appropriées pour que les acteurs du secteur privé dont les activités ont des effets extraterritoriaux, notamment les plateformes numériques, soient responsables des activités qu'ils mènent dans l'environnement numérique. Les États doivent exercer un contrôle adéquat sur les entreprises et les plateformes numériques relevant de leur compétence, faute de quoi il sera considéré qu'ils portent sciemment atteinte à la souveraineté nationale, à la sécurité et à l'ordre public d'autres États.

- Les États devraient empêcher les chaînes d'approvisionnement numériques développées sous leur contrôle et leur juridiction de créer ou d'aider à élaborer des produits, des services et une maintenance présentant des vulnérabilités qui compromettent la souveraineté et la protection des données d'autres États, et devraient s'abstenir d'utiliser ces chaînes.

Japon

Le Japon propose au Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale d'ajouter les passages suivants au texte d'orientations visant à mettre en œuvre la norme figurant à l'alinéa i) du paragraphe 13 relative à la garantie de l'intégrité de la chaîne d'approvisionnement :

- « Les États ont le droit et la responsabilité d'utiliser des fournisseurs et des vendeurs d'équipements et de systèmes informatiques qui soient dignes de confiance, notamment afin de garantir la sécurité nationale et la protection de la vie privée. Les mesures raisonnables à envisager peuvent inclure des mesures législatives ou administratives visant à assurer la sécurité de la chaîne d'approvisionnement, à appuyer le développement de technologies et d'industries fiables et dignes de confiance et à diversifier les fournisseurs. »

Pays-Bas

- « Les acteurs étatiques et non étatiques ne devraient ni mener ni permettre sciemment des activités qui portent intentionnellement et considérablement atteinte à la disponibilité générale ou à l'intégrité du cœur public d'Internet et, par conséquent, à la stabilité du cyberespace » [serait] une orientation à considérer pour la mise en œuvre de la norme figurant à l'alinéa f) du paragraphe 13 du rapport établi en 2015 par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale qui, par voie de conséquence, concernerait également la norme figurant à l'alinéa g) du paragraphe 13.

• « Les acteurs étatiques et non étatiques ne doivent pas mener, appuyer ou permettre des cyberopérations qui visent à perturber l'infrastructure technique essentielle aux élections, aux référendums ou aux plébiscites », [serait] une orientation à considérer pour la mise en œuvre de la norme figurant à l'alinéa f) du paragraphe 13 du rapport établi en 2015 par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale qui, par voie de conséquence, concernerait également la norme figurant à l'alinéa g) du paragraphe 13.

Mouvement des pays non alignés

• Les États Membres devraient être encouragés à compiler et à rationaliser les informations qu'ils ont présentées concernant leur mise en œuvre des règles internationales et le projet de répertoire qui s'y rapporte, en vue de réglementer les aspects spécifiques de l'utilisation des technologies de l'information et des communications par les États dans le contexte de la sécurité internationale et de recenser les domaines de préoccupation mutuelle.

• Les États Membres ne devraient pas mener ou soutenir sciemment des activités informatiques qui endommagent ou compromettent intentionnellement l'utilisation et le fonctionnement des infrastructures critiques d'autres États Membres, en violation du droit international.

• Il faudrait demander aux États Membres d'échanger des informations sur les vulnérabilités liées aux technologies de l'information et des communications et sur les fonctionnalités néfastes dissimulées dans les produits numériques, et d'avertir les utilisateurs lorsque des vulnérabilités importantes sont détectées.

• Les États Membres devraient également tenir compte de la résolution 73/27 de l'Assemblée générale dans toutes leurs activités informatiques.

• Le Mouvement des pays non alignés réaffirme sa vive préoccupation face au recours croissant à l'unilatéralisme et, à cet égard, souligne que le multilatéralisme et les solutions convenues dans un cadre multilatéral sont, conformément à la Charte des Nations Unies, la seule méthode viable pour traiter les questions de sécurité internationale.

• Le Mouvement des pays non alignés réaffirme que les États devraient s'abstenir de recourir à la menace ou à l'emploi de la force contre l'intégrité territoriale ou l'indépendance politique de tout État dans l'environnement numérique.

• Le Mouvement des pays non alignés appelle à l'intensification des efforts visant à éviter que le cyberespace devienne le théâtre de conflits et à garantir au contraire des utilisations exclusivement pacifiques qui permettraient de réaliser pleinement le potentiel des technologies de l'information et des communications pour contribuer au développement social et économique des pays.

• Le Mouvement des pays non alignés souligne qu'il importe de ne pas imposer de restrictions indues, y compris au moyen de mesures coercitives unilatérales, aux utilisations pacifiques des technologies de l'information et des communications, à la coopération internationale ou au transfert de technologies.

• Le Mouvement des pays non alignés souligne que les États ont la responsabilité première de maintenir un environnement numérique ouvert, sûr, stable, accessible et pacifique.

• Le Mouvement des pays non alignés souligne également qu'aucun État ne devrait mener ou soutenir sciemment des activités informatiques contraires aux obligations qui lui incombe en vertu du droit international, y compris celles qui

endommagent ou compromettent intentionnellement l'utilisation et le fonctionnement des infrastructures critiques.

Pakistan

- Les États Membres devraient être encouragés à continuer d'envisager, selon qu'il convient, l'adoption éventuelle d'un ou de plusieurs instruments juridiquement et politiquement contraignants afin de réglementer certains aspects de l'utilisation des technologies de l'information et des communications par les États dans le contexte de la sécurité internationale.

- Les États Membres devraient être encouragés à parvenir à une définition commune de ce qui constitue une « infrastructure critique », en vue de s'accorder sur l'interdiction des activités informatiques qui endommagent intentionnellement des infrastructures essentielles ou qui compromettent l'utilisation et le fonctionnement d'infrastructures essentielles.

- Les États Membres devraient être encouragés à coopérer pour parvenir à un accord sur l'interdiction de la dissimulation de fonctionnalités malveillantes ou de l'accumulation de vulnérabilités dans les produits numériques, ainsi qu'à s'engager à signaler de manière responsable les failles informatiques et à partager les informations correspondantes sur les moyens permettant d'y remédier.

- Les États Membres devraient s'efforcer de faciliter la coopération avec les fournisseurs de produits et services numériques afin d'empêcher l'exploitation ou l'utilisation abusive des données et de la vie privée des utilisateurs.

- Les États Membres devraient s'engager à ne pas utiliser les technologies de l'information et des communications pour mener des activités contraires au maintien de la paix et de la sécurité internationales, et s'abstenir d'utiliser ces technologies pour s'ingérer de quelque manière que ce soit dans les affaires intérieures d'autres États.

- Les États Membres devraient coopérer pour remédier aux difficultés que pose l'attribution des responsabilités dans le domaine du numérique. L'adoption d'une stratégie commune élaborée dans un cadre universel sous les auspices de l'ONU reste le moyen le plus efficace d'avancer à cet égard.

- Il faut exhorter les États Membres à parvenir à un accord sur l'interdiction des activités informatiques qui visent à perturber l'infrastructure technique essentielle aux élections, aux référendums ou aux plébiscites.

- Les États Membres devraient être encouragés à élaborer et à appliquer des normes d'une manière qui évite de restreindre indûment les utilisations pacifiques des technologies de l'information et des communications, la coopération internationale ou le transfert de technologies.

République de Corée

Les orientations suivantes sont proposées pour la mise en œuvre de la norme figurant à l'alinéa c) du paragraphe 13 du rapport établi en 2015 par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale :

- Lorsqu'un État touché avise un autre État, au moyen d'informations fiables, que des incidents informatiques ont émané de son territoire ou le concernent, l'État qui reçoit un tel avis doit, conformément au droit international et national et dans la limite

de ses capacités, prendre toutes les mesures raisonnables, sur son territoire, pour faire cesser ces activités ou en atténuer les conséquences.

- Il doit être entendu que le fait d'aviser un État n'implique pas la responsabilité de cet État dans l'incident.

- Ces informations devraient inclure au minimum les éléments révélateurs d'une intrusion, tels que l'adresse de protocole Internet, la localisation des auteurs et des ordinateurs utilisés pour commettre des actes malveillants et des informations sur les logiciels malveillants.