



Assemblée générale

Distr. générale
18 avril 2023
Français
Original : anglais

Soixante-dix-huitième session
Point 97 de la liste préliminaire*
Progrès de l'informatique et des télécommunications
et sécurité internationale

Programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale

Rapport du Secrétaire général

Résumé

Faisant la synthèse des communications reçues des États Membres comme suite à la résolution [77/37](#) de l'Assemblée générale, sans préjudice de la position de chacun d'eux sur la question, le présent rapport recense leurs vues sur la portée, la structure, les principes, la teneur, les travaux préparatoires et les modalités de mise en place du programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale.

* [A/78/50](#).



Table des matières

	<i>Page</i>
I. Introduction	2
II. Historique	4
III. Portée, structure et principes	6
IV. Teneur, travaux préparatoires et modalités de mise en place	8
V. Fonctions	9
VI. Mécanisme de suivi et mise en œuvre	11
VII. Observations et conclusions du Secrétaire général	12
Annexe	
Réponses reçues	15
Albanie	15
Allemagne	16
Australie	19
Autriche	23
Belgique	24
Canada	27
Chili	32
Colombie	34
Cuba	36
Danemark	37
Égypte	39
El Salvador	43
Équateur	46
Estonie	47
États-Unis d'Amérique	49
Fédération de Russie	53
Finlande	55
France	59
Italie	64
Japon	67
Lettonie	70
Macédoine du Nord	72
Monaco	74
Norvège	75
Nouvelle-Zélande	76

Pakistan	77
Pays-Bas (Royaume des)	78
Philippines	82
Roumanie	83
Royaume-Uni de Grande-Bretagne et d'Irlande du Nord	84
Singapour	87
Slovénie	88
Suède	89
Suisse	92
Tchéquie	94
Türkiye	97
Ukraine	98

I. Introduction

1. Au paragraphe 3 de sa résolution 77/37, l'Assemblée générale a prié le Secrétaire général de solliciter les vues des États Membres sur la portée, la structure et la teneur du programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, ainsi que sur les travaux préparatoires et les modalités de mise en place de ce mécanisme, notamment dans le cadre d'une conférence internationale, en tenant compte de sa résolution 76/19, des rapports de consensus de 2010¹, 2013², 2015³ et 2021⁴ des groupes d'experts gouvernementaux, du rapport de 2021 du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale⁵, du premier rapport d'activité annuel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025)⁶, des vues et des propositions présentées par les États Membres dans le cadre du groupe de travail à composition non limitée (2021-2025) et des consultations régionales tenues conformément au paragraphe 4 de sa résolution 77/37, et d'établir à partir de ces informations un rapport qu'il lui présentera à sa soixante-dix-huitième session et qui sera également examiné par les États Membres lors des réunions du groupe de travail à composition non limitée (2021-2025). Le présent rapport fait suite à cette demande.

2. Le 14 décembre 2022, le Bureau des affaires de désarmement du Secrétariat a communiqué une note verbale à tous les États Membres dans laquelle il appelait leur attention sur le paragraphe 3 de la résolution 77/37 de l'Assemblée générale et sollicitait leurs vues sur la question. Par la suite, la date limite de présentation des communications a été reportée et communiquée dans une note verbale datée du 3 mars 2023. On trouvera dans l'annexe au présent rapport le texte des communications exposant les vues reçues d'États Membres au 14 avril 2023. Les points de vue reçus après cette date ont été publiés sur la page Web des réunions du Bureau des affaires de désarmement⁷.

3. Les sections III à VI du présent rapport font la synthèse des communications reçues des États Membres, sans préjudice de la position de chacun d'eux sur la question, la section VII étant consacrée aux conclusions et observations du Secrétaire général.

II. Historique

4. Dans sa résolution 77/37, l'Assemblée générale s'est félicitée de la proposition de créer un programme d'action des Nations Unies destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. Dans la même résolution, l'Assemblée a souligné que le projet de programme d'action et les travaux menés par l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) étaient complémentaires, et réaffirmé que tout futur processus de dialogue institutionnel régulier mis en place sous les auspices des Nations Unies sur

¹ A/65/201.

² A/68/98.

³ A/70/174.

⁴ A/76/135.

⁵ A/75/816.

⁶ A/77/275.

⁷ Voir <https://meetings.unoda.org/ga-cl/general-assembly-first-committee-seventy-eighth-session-2023>.

la sécurité du numérique devrait être orienté vers l'action et assorti d'objectifs spécifiques, s'appuyer sur les réalisations précédentes et être inclusif, transparent, fondé sur le consensus et axé sur les résultats.

5. Dans sa résolution 77/37, l'Assemblée générale a décrit le programme d'action comme un mécanisme permanent, inclusif et orienté vers l'action, qui sera doté de plusieurs fonctions, dont les suivantes :

- a) examiner les menaces existantes et potentielles ;
- b) renforcer les capacités des États et appuyer les efforts faits par les États pour mettre en œuvre et promouvoir les engagements pris au titre du cadre de comportement responsable des États, qui comprend des normes volontaires et non contraignantes en matière d'application du droit international à l'utilisation des technologies numériques par les États, ainsi que des mesures de confiance et de renforcement des capacités ;
- c) étudier ce cadre et le développer, le cas échéant ;
- d) promouvoir le dialogue et la coopération avec les parties concernées ;
- e) examiner périodiquement les progrès accomplis dans la mise en œuvre du programme d'action ainsi que les futurs travaux devant être entrepris dans ce contexte.

6. Le projet de programme d'action a été présenté pour la première fois par un groupe de coauteurs⁸ en décembre 2020 sous les auspices du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui a tenu des sessions de 2019 à 2021, sous le thème « Dialogue institutionnel régulier ». Une note de cadrage sur les aspects organisationnels d'un programme d'action a été diffusée ainsi qu'un projet de texte pour inclusion dans le rapport final du Groupe de travail (voir tableau ci-dessous)⁹.

7. À la suite de sa présentation initiale en décembre 2020, le projet de programme d'action a été examiné dans le cadre de processus intergouvernementaux ultérieurs. Les États sont convenus de continuer d'examiner ce projet sous les auspices du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). De nombreux États ont présenté diverses propositions et réflexions concernant le programme d'action lors des débats au titre du point de l'ordre du jour intitulé « Dialogue institutionnel régulier ».

Termes de consensus relatifs au projet de programme d'action

<i>Cote du document</i>	<i>Titre du document</i>	<i>Par./sect.</i>
A/75/816	Rapport du Groupe de travail à composition non limitée sur les progrès de l'informatique et des	Paragraphe 77

⁸ Argentine, Canada, Colombie, Égypte, El Salvador, Émirats arabes unis, Équateur, Gabon, Géorgie, Islande, Japon, Liban, Macédoine du Nord, Maroc, Monténégro, Norvège, République de Corée, République de Moldova, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Singapour et l'Union européenne et les États membres de l'Union européenne (Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Suède et Tchéquie).

⁹ Voir <https://front.un-arm.org/wp-content/uploads/2020/12/sponsors-oewg-concept-note-final-12-2-2020.pdf>.

<i>Cote du document</i>	<i>Titre du document</i>	<i>Par./sect.</i>
	télécommunications dans le contexte de la sécurité internationale	
A/77/275	Rapport du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), annexe intitulée « Rapport d'activité sur les débats du groupe de travail tenus au titre du point 5 de l'ordre du jour »	Section G, paragraphe 18 b) Section G, Prochaines étapes recommandées, paragraphe 2

III. Portée, structure et principes

Portée

8. Dans leurs communications, de nombreux États ont souligné qu'il importait de préserver la paix, la sécurité et la stabilité dans l'environnement numérique et noté que l'objectif général de tout dialogue institutionnel régulier consacré à l'utilisation du numérique par les États dans le contexte de la sécurité internationale était d'y contribuer. Les débats sur le projet de programme d'action ayant eu lieu sous les auspices de la Première Commission de l'Assemblée générale, de nombreux États ont souligné que la portée du programme d'action devrait s'inscrire dans le cadre du maintien de la paix et de la sécurité internationales en préservant un environnement numérique ouvert, stable, sûr, accessible et pacifique. Plusieurs États ont fait remarquer qu'un programme d'action pourrait fournir un cadre général aux initiatives en matière de cybersécurité. Quelques États ont mentionné précisément les objectifs de coopération, de stabilité et de résilience dans ce contexte. Un certain nombre d'États ont souligné le rôle que pourrait jouer le programme d'action dans la prévention des conflits et la promotion de l'utilisation du numérique à des fins pacifiques.

9. De nombreux États ont noté que l'objectif principal du programme d'action devrait être de soutenir la mise en œuvre concrète du cadre de comportement responsable des États en matière d'utilisation du numérique, tel qu'approuvé par consensus par l'Assemblée générale dans sa décision 75/564 du 28 avril 2021. Plusieurs États ont qualifié ce cadre d'« évolutif et cumulatif », notant que le programme d'action devrait permettre d'assurer le développement futur du cadre, en particulier face aux nouvelles menaces et aux nouveaux défis qui pourraient se poser dans le cyberspace. En ce qui concerne le cadre, plusieurs États l'ont défini comme étant composé à la fois des normes de comportement responsable des États, de l'applicabilité du droit international à l'utilisation du numérique par les États, des mesures de confiance et du renforcement des capacités.

10. En ce qui concerne la mise en œuvre du cadre normatif, un certain nombre d'États ont souligné que le renforcement des capacités, notamment l'aide financière et l'assistance technique, devrait être un élément fondamental du programme d'action et soutenir la capacité des États à remplir leurs engagements. Quelques États ont noté que le programme d'action devrait renforcer les effets de synergie avec l'action menée dans d'autres domaines, notamment dans le développement numérique.

11. On a fait valoir qu'un mécanisme relatif à un dialogue institutionnel régulier sur la sécurité du numérique devrait inclure l'élaboration d'un instrument juridiquement contraignant qui compléterait le droit international applicable et ferait face efficacement aux menaces croissantes. À cet égard, certains États ont dit qu'ils

doutaient qu'un programme d'action politiquement contraignant puisse contribuer à ce que les États mettent en œuvre le cadre normatif et en rendent compte. On a fait observer qu'en l'absence de dispositions juridiquement contraignantes, le programme d'action pourrait décourager la formulation éventuelle d'un futur instrument juridiquement contraignant. D'autres propositions relatives à un dialogue institutionnel régulier présentées dans le cadre du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) ont été mentionnées, notamment une convention des Nations Unies sur la sécurité internationale de l'information.

Structure

12. Les États ont noté qu'il était d'une importance cruciale que les débats consacrés à leur utilisation du numérique dans le contexte de la sécurité internationale se déroulent sous les auspices des Nations Unies. À cet égard, il a été généralement admis que tout débat sur un futur dialogue institutionnel régulier devrait être mené dans le cadre de l'ONU. Plusieurs États ont noté que la Première Commission de l'Assemblée générale était l'instance la plus appropriée pour faire avancer ces débats.

13. Plusieurs États ont demandé que le programme d'action soit inscrit dans une déclaration politique devant être adoptée par l'Assemblée générale, par laquelle, entre autres choses : a) les États réaffirmeraient leur attachement au cadre de comportement responsable des États, tel qu'il a été énoncé dans les rapports et les résolutions adoptés par consensus ; b) un mécanisme institutionnel permanent pourrait être mis en place pour faire progresser la mise en œuvre du cadre, en poursuivre le développement, le cas échéant, et favoriser la coopération multipartite dans les domaines concernés.

Principes

14. De nombreux États ont rappelé la conclusion du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, selon laquelle tout futur processus de dialogue institutionnel régulier 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. Dans leurs communications, de nombreux États ont souligné que ces principes devraient sous-tendre le programme d'action.

15. De nombreux États ont insisté sur le fait qu'il était capital de prendre des décisions par consensus. Un certain nombre d'États ont noté, en particulier, que, dans le cadre du programme d'action, les décisions relatives aux questions de fond devaient être adoptées par consensus. En ce qui concerne la possibilité d'actualiser le cadre normatif au moyen du programme d'action, plusieurs États ont souligné que de telles décisions devaient être prises par consensus. Dans ce contexte, plusieurs États ont soutenu l'application des principes de souplesse et d'adaptabilité pour permettre au cadre de faire face à l'avenir à de nouveaux défis.

16. Les États ont dégagé d'autres principes dans leurs communications, notamment la permanence, la neutralité, la légitimité, la pérennité, la politique des petits pas, la continuité et la stabilité. En ce qui concerne la permanence, certains États ont fait remarquer que la permanence d'une structure relative au programme d'action assurerait la stabilité institutionnelle et permettrait à l'Assemblée générale d'économiser du temps et des ressources, car elle n'aurait pas à négocier de nouveaux mandats.

17. De nombreux États considèrent qu'il importe grandement que de multiples parties prenantes participent à l'élaboration du programme d'action. Plusieurs États

ont rappelé que, bien qu'il incombait exclusivement aux États de négocier les recommandations et de prendre des décisions, les échanges avec les parties prenantes concernées, notamment les organisations régionales et sous-régionales, la société civile, le secteur privé et le monde universitaire, étaient d'une très grande utilité. Ces États ont demandé que les modalités de participation associent toutes les parties. On a fait valoir que le caractère intergouvernemental du programme d'action devrait être préservé. D'autres États ont noté qu'on devrait nouer une collaboration avec les organisations régionales et sous-régionales, notamment pour ce qui était de tirer parti de leur compétences spécialisées, afin d'éviter les doubles emplois.

18. Quelques États ont souligné qu'il importait d'instaurer un environnement favorable à la réduction de la fracture numérique, notamment à celle des disparités entre les sexes dans le domaine du numérique. Un appel a été lancé pour favoriser la participation effective et véritable des femmes aux processus décisionnels liés à la sécurité du numérique, et leur influence.

IV. Teneur, travaux préparatoires et modalités de mise en place

Teneur

19. Dans leurs communications, les États ont réfléchi de diverses manières à une teneur du programme d'action qui permettrait de promouvoir, d'affiner et de mettre en œuvre des positions communes et des mesures de coopération en matière d'utilisation du numérique par les États dans le contexte de la sécurité internationale.

20. Les États ont présenté un ensemble de propositions visant à inclure tel ou tel élément dans le programme d'action, dont des mesures et des engagements dont l'objectif était de mettre en œuvre concrètement le cadre normatif. On comptait notamment des propositions relatives à un « système de classement » pour ce qui était d'approuver et de promouvoir des activités sur le renforcement des capacités qui s'inscrivaient dans le prolongement des objectifs du programme d'action, à l'élaboration d'une procédure de soumission de demandes d'assistance internationale, à un programme de bourses, à un mécanisme de partenariat interrégional et à un fonds d'affectation spéciale. En ce qui concerne la dernière proposition, plusieurs États ont examiné, à titre d'exemple, des mécanismes des Nations Unies en vigueur dans le domaine de la maîtrise des armements, tels que le Mécanisme de financement des Nations Unies pour la coopération en matière de réglementation des armements et le fonds appelé « Entité "Sauver des vies" ». Des États ont mentionné d'autres structures de financement, telles que le Fonds d'affectation spéciale multidonateur de la Banque mondiale pour la cybersécurité, ainsi que celles qui existaient aux niveaux régional et sous-régional.

Travaux préparatoires

21. Les États ont rappelé l'importance des travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et le rôle essentiel qu'il jouait pour ce qui était de soutenir les débats relatifs à l'élaboration de tout futur dialogue institutionnel régulier. De nombreux États ont souligné le rôle important qu'il jouait également pour ce qui était de poursuivre l'élaboration du projet de programme d'action. Un certain nombre d'États ont souligné que l'élaboration du programme d'action ne devrait être engagée qu'à l'issue du mandat du groupe de travail et que sa mise en place devrait être décidée par consensus sous les auspices du groupe de travail.

22. Plusieurs États ont indiqué qu'ils trouvaient problématique la création de voies parallèles car celles-ci mobiliseraient trop de ressources, déjà limitées, et

présenteraient des difficultés pour les délégations, en particulier pour les délégations de plus petite taille des pays en développement. À cet égard, des États ont déclaré que les débats relatifs au projet de programme d'action devraient se poursuivre exclusivement dans le cadre du groupe de travail, qui constituait l'instance appropriée pour examiner toutes les propositions des États, compte tenu de son caractère inclusif et de son processus de prise de décision fondé sur le consensus. On a fait valoir que la décision des États quant à un futur mécanisme de dialogue institutionnel des Nations Unies sur la sécurité du numérique ne devrait pas être prédéterminée par le programme d'action et que le projet de programme d'action ainsi que toutes les autres propositions des États devraient être débattus dans le cadre du groupe de travail, conformément à son mandat énoncé dans la résolution 75/240 de l'Assemblée générale.

23. Certains États ont noté que les vues et les contributions des États présentées sous les auspices du groupe de travail concernant le programme d'action ainsi que le présent rapport du Secrétaire général présenté en application de la résolution 77/37 de l'Assemblée générale devraient servir à établir la portée, la structure et la teneur du programme d'action. À cet égard, de nombreux États ont demandé que d'autres débats soient consacrés à l'élaboration du projet de programme d'action lors des réunions du groupe de travail, dont des sessions spéciales en 2024 et 2025, et qu'il soit possible de convoquer des réunions intersessions supplémentaires.

Modalités de mise en place

24. De nombreux États ont rappelé la référence faite dans la résolution 77/37 de l'Assemblée générale à la possibilité d'organiser une conférence internationale pour soutenir la mise en place du programme d'action. Un certain nombre d'États ont accueilli favorablement l'organisation d'une telle conférence à l'issue des travaux de l'actuel groupe de travail, en 2025. Il a été suggéré de convoquer la conférence internationale immédiatement après la dernière session du groupe de travail, en 2025, et d'organiser régulièrement des réunions de suivi du programme d'action à partir de 2026. On a fait valoir que la conférence internationale devrait être convoquée au plus tard en août 2024. Il a été noté qu'une décision concernant la conférence internationale dépendrait des vues et des analyses des États Membres, présentées dans le présent rapport, quant à la nécessité de l'organisation d'une telle conférence.

25. Dans leurs communications, les États ont évoqué le rôle que jouerait une conférence internationale, notamment en ce qui concerne l'adoption d'un document fondateur du programme d'action sur la base des travaux préparatoires entrepris sous les auspices du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Plusieurs États ont demandé que la conférence internationale prévoie la participation des parties prenantes et prenne des décisions sur la base d'un consensus, au moins sur les questions de fond.

26. Un certain nombre d'États ont soutenu l'idée selon laquelle le programme d'action pourrait être présenté dans le cadre d'une déclaration politique qui serait adoptée lors de la conférence internationale et ensuite approuvée par l'Assemblée générale.

V. Fonctions

27. Dans leurs communications, les États ont recensé diverses fonctions qui pourraient être exercées et diverses activités qui pourraient être menées dans le cadre du futur programme d'action, notamment celles liées à l'échange d'informations sur, entre autres, les menaces existantes et potentielles et les moyens d'y faire face ; les exercices concrets et les échanges entre les équipes d'intervention informatique

d'urgence ; les débats sur le droit international, le renforcement des capacités et les mesures de confiance.

28. Un certain nombre d'États ont indiqué qu'il fallait que, dans le cadre du programme d'action, on recense les lacunes du cadre normatif existant et qu'on envisage des recommandations pratiques pour soutenir les efforts de mise en œuvre. On a fait valoir que, pour combler les lacunes et faire face aux défis, les États pourraient envisager de nouvelles normes, règles et principes, ainsi que des obligations juridiquement contraignantes, afin de faire progresser la mise en œuvre du cadre convenu.

29. Dans le domaine du droit international, plusieurs États ont déclaré que le programme d'action pourrait constituer un cadre inclusif dans lequel poursuivre les débats sur l'applicabilité du droit international à l'utilisation du numérique par les États et renforcer les positions communes sur la question, notamment dans le cadre d'un axe de travail dédié. Dans ce contexte, certains États ont encouragé les pays à faire connaître leur position quant à la manière dont le droit international s'appliquait au cyberspace.

30. En ce qui concerne l'échange d'informations, y compris les données d'expérience nationales, il a été proposé que les États procèdent à une auto-évaluation en vue de mettre en commun les bonnes pratiques. À cet égard, plusieurs États ont fait remarquer qu'il existait des outils pour réaliser à titre volontaire une évaluation des progrès accomplis dans la mise en œuvre, tels que l'enquête sur l'application à l'échelle nationale des recommandations de l'Organisation des Nations Unies en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale, disponible sur le Portail des politiques de cybersécurité de l'Institut des Nations Unies pour la recherche sur le désarmement¹⁰.

31. De nombreux États ont souligné que le renforcement des capacités devrait être une fonction centrale du programme d'action. Un certain nombre d'États ont rappelé les directives relatives au renforcement des capacités adoptées par consensus dans 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.

32. Plusieurs États ont souligné l'intérêt de tirer parti des efforts existants mis en œuvre par des organisations régionales et l'Institut des Nations Unies pour la recherche sur le désarmement, ainsi que par de multiples parties prenantes, tels que ceux entrepris dans le cadre du Forum mondial sur la cyber expertise. D'aucuns ont souligné l'intérêt de la participation des parties prenantes dans le domaine du renforcement des capacités et noté la possibilité de faire correspondre les besoins et les ressources. Un État a proposé la mise en place d'un mécanisme concret pour favoriser le renforcement des capacités, à savoir un cycle en quatre étapes consistant à : a) élaborer un ensemble de domaines pour le renforcement des capacités ; b) procéder à une auto-évaluation des besoins ; c) faire correspondre les besoins et les ressources ; d) mettre en place un retour d'expérience.

33. Le rôle du programme d'action dans l'instauration de la confiance, notamment au moyen de mesures de confiance concrètes, a été souligné. À cet égard, certains États ont rappelé la décision prise par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) d'établir un répertoire intergouvernemental mondial d'interlocuteurs, qui pourrait jouer un rôle dans l'élaboration de mesures de confiance supplémentaires.

¹⁰ <https://nationalcybersurvey.cyberpolicyportal.org/>.

34. Rappelant les principes de souplesse et d'adaptabilité, plusieurs États ont noté le rôle du programme d'action pour ce qui était de promouvoir une position commune quant aux menaces existantes et potentielles et à la manière d'y faire face. Certains États ont souligné qu'il importait d'échanger des informations sur ces questions, notamment sur les faiblesses et la protection des infrastructures critiques, y compris dans le contexte des services de soins de santé et des services médicaux. En outre, en ce qui concerne les nouvelles menaces, plusieurs États ont noté que le programme d'action devrait permettre de poursuivre le développement du cadre, le cas échéant, sur la base d'un consensus.

VI. Mécanisme de suivi et mise en œuvre

35. Dans leurs communications, de nombreux États ont réfléchi à la forme, à la fréquence et à l'objectif que prendrait un mécanisme de suivi du programme d'action. De nombreux États se sont dits pour l'organisation de réunions officielles afin de débattre de la mise en œuvre et de l'évolution du cadre relatif au programme d'action. Certains se sont prononcés en faveur de réunions annuelles, tandis que d'autres ont évoqué la possibilité de réunions biennales. D'autres États se sont dits souples quant à la fréquence de ces réunions. En ce qui concerne le lieu, plusieurs États ont soutenu la tenue des réunions de suivi à New York, quelques-uns évoquant la possibilité d'organiser des réunions dans d'autres lieux, comme à Genève. De nombreux États ont souligné qu'il importait que toutes les décisions soient prises sur la base d'un consensus lors de ces réunions de suivi et que les efforts de mise en œuvre soient examinés lors de réunions de suivi officielles.

36. Un certain nombre d'États ont évoqué la possibilité de tenir des conférences d'examen, avec des fréquences diverses, de tous les trois à quatre ans à tous les six ans. Un certain nombre d'États ont indiqué que la conférence d'examen serait l'instance adéquate dans laquelle examiner la possible mise en adéquation du cadre du programme d'action avec les nouvelles menaces. Plusieurs États ont noté que les conférences d'examen serviraient de mécanisme pour ce qui est de déterminer les priorités et les axes de travail durant la période intermédiaire, y compris l'élaboration éventuelle d'un programme de travail.

37. De manière à soutenir les travaux intersessions, un certain nombre d'États ont demandé la création d'axes de travail techniques, de groupes de travail sur tel ou tel sujet et d'autres formes de réunions consultatives intersessions. À cet égard, plusieurs États ont souligné que les décisions relatives à la création de ces groupes de travail devraient être prises lors des réunions plénières de suivi, notamment des conférences d'examen. On a fait valoir que les groupes de travail techniques pourraient être convoqués dans un format hybride ou virtuel afin de permettre la participation la plus large possible d'experts. Au nombre des thèmes suggérés pour les groupes de travail possibles figuraient notamment l'applicabilité du droit international, la mise en œuvre de telle ou telle norme de comportement responsable des États et l'élaboration de nouvelles normes, règles ou principes, notamment d'obligations ou d'instruments juridiquement contraignants, le cas échéant. Il a également été suggéré que les groupes de travail se penchent sur des thèmes tels que la protection des infrastructures critiques.

38. De nombreux États ont noté l'intérêt d'un mécanisme de communication de l'information à titre volontaire et la manière dont celui-ci pourrait soutenir la mise en œuvre du programme d'action et les efforts de renforcement des capacités y relatives. Plusieurs États ont rappelé que l'enquête sur l'application à l'échelle nationale des recommandations de l'Organisation des Nations Unies en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale

était un outil pertinent à cet égard. Certains États ont fait part de leur intérêt pour la tenue de débats sur un modèle standard de communication de l'information. Il a été suggéré que la communication annuelle de l'information prenne la forme d'une enquête, ceci devant faire l'objet d'un consensus, qui serait d'un abord facile et administrée dans le cadre d'une plateforme en ligne. Certains États ont fait remarquer que la communication de l'information à titre volontaire pourrait contribuer à recenser les priorités en matière de mise en œuvre et à définir les besoins relatifs au renforcement des capacités.

39. Un certain nombre d'États ont noté que le Bureau des affaires de désarmement serait l'entité la plus adéquate pour assurer le secrétariat du programme d'action. Quelques États ont noté le rôle possible de l'Institut des Nations Unies pour la recherche sur le désarmement dans le soutien à la mise en œuvre du programme d'action, notamment par le biais d'activités de recherche pertinentes.

40. En ce qui concerne le mécanisme de suivi et de mise en œuvre du programme d'action, de nombreux États ont souligné l'intérêt d'une participation inclusive des parties prenantes non gouvernementales, notamment de la société civile, du secteur privé, du monde universitaire et de la communauté technique, et demandé que les modalités de leur participation soient bien déterminées. Plusieurs États ont indiqué que les parties prenantes devraient participer aux réunions de suivi du programme d'action et apporter des contributions par écrit et oralement. Certains États ont donné des exemples précis des modalités relatives à la participation des parties prenantes, notamment celles convenues dans le cadre du Groupe de travail à composition non limitée sur le vieillissement, du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles et du groupe d'experts gouvernementaux chargé d'étudier les questions ayant trait aux technologies émergentes dans le domaine des systèmes d'armes létaux autonomes des Hautes Parties contractantes à la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination. On a fait valoir que les modalités convenues pour le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) devraient former la base des modalités de participation en ce qui concerne le programme d'action.

VII. Observations et conclusions du Secrétaire général

41. Il est primordial d'instaurer un environnement pacifique, stable et sûr pour le numérique, dans lequel les droits humains et les libertés fondamentales sont respectés et protégés. La communauté internationale fait face à des défis extraordinaires pour atteindre cet objectif. Au cours des dernières décennies, l'ampleur, l'étendue et la fréquence de l'utilisation malveillante du numérique s'est considérablement accrue. Il est largement admis que, outre l'utilisation malveillante du numérique par des acteurs non étatiques, un certain nombre d'États développent des capacités numériques à des fins militaires. La nécessité d'agir sans tarder pour ce qui est de renforcer la sûreté et la sécurité de l'environnement numérique, notamment de renforcer la protection des civils contre les activités malveillantes, s'est accrue de manière exponentielle. Les incidents malveillants en matière de numérique ayant eu une incidence sur les infrastructures de services au public essentielles au fonctionnement de la société, y compris l'énergie et le secteur des soins de santé, ont été amplement démontrés.

42. L'environnement du numérique n'est pas un espace de non-droit. L'état de droit existe dans la sphère numérique comme dans le monde physique. Les États ont

affirmé que le droit international, en particulier la Charte des Nations Unies, s'appliquait à l'utilisation du numérique par les États. À la suite des travaux assidus entrepris sous les auspices de l'Assemblée générale durant les deux dernières décennies, tous les États ont accepté d'être guidés dans leur utilisation du numérique par des normes de comportement responsable précisément définies. Ce cadre normatif, qui s'appuie sur une affirmation universelle de l'applicabilité du droit international et un engagement en faveur de mesures de confiance et de renforcement des capacités, représente une étape importante en matière de coopération internationale en vue de l'instauration d'un environnement numérique ouvert, sûr, stable, accessible et pacifique. Ces progrès ont été durement acquis et doivent servir de point de départ à tous les travaux multilatéraux futurs dans ce domaine.

43. Dans des moments comme celui-ci, nous devons mesurer l'importance cruciale des normes, règles et principes communs pour ce qui est de préserver la paix et la sécurité de l'environnement numérique et redoubler d'efforts pour les mettre en œuvre. Nous nous félicitons de l'examen des projets de mécanisme orienté vers l'action s'agissant de faire progresser la mise en œuvre du cadre normatif universellement approuvé pour un comportement responsable des États et de soutenir les capacités des États à le mettre en œuvre. À cet égard, l'examen d'une manière inclusive et transparente du projet de programme d'action, qui serait fermement ancré dans les accords de consensus antérieurs et les progrès réalisés dans le cadre de l'Assemblée générale, est une entreprise qui en vaut la peine.

44. Les États continuent de réaffirmer que l'instauration d'un dialogue institutionnel régulier sous les auspices des Nations Unies soutient les objectifs communs de renforcement de la paix et de la stabilité internationales et de prévention des conflits dans l'environnement numérique. Ils ont conclu qu'à la lumière de l'ampleur des menaces émanant de l'utilisation malveillante du numérique, il fallait renforcer d'urgence la position commune, instaurer la confiance et resserrer la coopération internationale. Ils ont également conclu que le dialogue institutionnel régulier sur ces questions devrait être inclusif, transparent, fondé sur le consensus et axé sur les résultats. Compte tenu du caractère dynamique des technologies de l'information et des communications et de l'évolution rapide de l'environnement numérique, la souplesse et l'adaptabilité sont des facteurs importants qu'il faut continuer à prendre en considération.

45. S'il est vrai que les progrès réalisés jusqu'à présent sont louables, nous devons rester vigilants et veiller à ce que les accords multilatéraux dans ce domaine soient adaptés aux nouvelles menaces et aux nouveaux défis. C'est dans cette optique qu'il convient d'examiner tous les projets de mécanisme des Nations Unies visant à promouvoir la paix et la sécurité dans l'environnement numérique.

46. Il existe un large consensus sur le fait que la prise de décision par consensus et l'inclusion, en particulier, sont des éléments essentiels d'un dialogue institutionnel régulier dans ce domaine. Il faut maintenir le caractère consensuel des débats multilatéraux sur la sécurité du numérique. De manière à garantir la participation la plus élevée possible, les États doivent tenir compte des préoccupations des délégations, en particulier de celles des délégations de plus petite taille des pays en développement, qui estiment que créer des voies parallèles sur les mêmes questions entraînerait une surcharge de travail et une trop grande mobilisation des ressources déjà limitées. En outre, compte tenu du caractère singulier du numérique et du rôle particulier que jouent les parties prenantes non gouvernementales pour ce qui est de soutenir la mise en œuvre des normes convenues, l'inclusivité doit s'appliquer à la participation et aux contributions adéquates des parties prenantes concernées, en gardant à l'esprit le droit exclusif des États en matière de prise de décision.

47. En ce qui concerne le programme d'action, ainsi que toutes les autres propositions faites par les États, les consultations permettant d'aboutir à un accord seront un facteur essentiel pour déterminer le niveau d'acceptation du programme d'action et, donc, sa mise en œuvre et son succès à long terme. À cet égard, le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), compte tenu de son rôle et de son caractère universel et consensuel, reste l'instance la plus appropriée pour continuer à élaborer le cadre du programme d'action et à donner une existence à ses divers éléments, tant sur le fond que sur la forme. Il existe un large consensus sur le fait que le groupe de travail devrait jouer un rôle clé dans la poursuite des travaux relatifs au projet de programme d'action et qu'il pourrait, dans le cadre de son mandat actuel, qui doit s'achever en 2025, faciliter des échanges supplémentaires sur le projet.

48. Bien que tous les États conviennent de la nécessité d'un dialogue institutionnel régulier sous les auspices des Nations Unies, tous ne considèrent pas le projet de programme d'action comme le seul mécanisme possible ou le mécanisme le plus approprié pour atteindre cet objectif. **Il est donc recommandé aux États de continuer d'examiner la portée, la structure, les principes, la teneur, les fonctions et le mécanisme de suivi possibles du projet de programme d'action sous les auspices du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), en s'appuyant sur les points de vue exprimés dans le présent rapport et en tenant compte des consultations régionales et sous-régionales organisées par le Bureau des affaires de désarmement en application de la résolution 77/37 de l'Assemblée générale. Les questions de procédure, y compris les crédits nécessaires, devraient également être examinés. En plus des débats tenus au titre du point de l'ordre du jour intitulé « Dialogue institutionnel régulier », une réunion intersession consacrée au projet de programme d'action pourrait être convoquée en 2024 ainsi qu'en 2025 afin de garantir que tous les points de vue soient exprimés. Lors de l'examen du projet de programme d'action, il est impératif que les États continuent à œuvrer en faveur d'un consensus. La participation active de l'ensemble des membres de l'Organisation des Nations Unies est essentielle au succès de cette entreprise.**

Annexe

Réponses reçues

Albanie

[Original : anglais]

[14 avril 2023]

Contribution du Gouvernement albanais au rapport du Secrétaire général sur le programme d'action pour la mise en œuvre du cadre et le renforcement de la résilience conformément à la résolution 77/37 de l'Assemblée générale des Nations Unies

En tout premier lieu, l'Albanie estime que l'Organisation des Nations Unies devrait disposer d'un instrument efficace si elle veut réussir à maintenir la paix et la stabilité dans le cyberspace ; elle fait donc part de son plein soutien à la mise en place d'un programme d'action.

Le Gouvernement albanais est conscient du rôle important que jouent la coopération et la collaboration internationales pour relever efficacement les défis en matière de cybersécurité. À cet égard, nous pensons que le programme d'action fournira un cadre à la coopération internationale et au dialogue sur la cybersécurité, notamment à l'échange des meilleures pratiques, à l'élaboration et à l'application des normes et principes existants et au renforcement des capacités et des compétences.

À l'heure où les progrès technologiques ont une incidence considérable sur la paix et la sécurité internationales et où le risque d'utilisation à mauvais escient par des États ou des acteurs non étatiques augmente considérablement, le programme d'action, en tant que mécanisme permanent, pourrait contribuer pour beaucoup à apporter résilience et stabilité dans le cyberspace.

L'Albanie s'est engagée à soutenir la mise en place du programme d'action et à participer activement à ses travaux. Nous exposerons donc nos attentes concernant la manière dont, en s'appuyant sur cinq principes clés, le programme d'action pourrait soutenir la mise en œuvre du cadre et renforcer les capacités des États et l'action qu'ils mènent pour développer la résilience :

- **Faciliter l'échange des meilleures pratiques** : nous escomptons que le programme d'action fournira aux États une plateforme pour qu'ils mettent en commun leurs expériences et leurs meilleures pratiques dans la mise en œuvre du cadre. Cela pourrait aider les États à apprendre les uns des autres, à recenser les bonnes pratiques et à mettre celles-ci en œuvre dans leur écosystème de cybersécurité.
- **Soutenir le renforcement des capacités** : le programme d'action devrait aider les États à renforcer leurs capacités à répondre aux cybermenaces et aux cyberattaques. Il pourrait s'agir de programmes de formation, d'assistance technique et d'autres formes de soutien visant à aider les États à renforcer leurs capacités de prévention, de détection et de réaction aux cyberincidents.
- **Faciliter et encourager l'application du droit international et des normes de comportement responsable des États dans le cyberspace** : le programme d'action devrait faciliter l'application des normes et principes de comportement responsable des États dans le cyberspace, assortie d'un suivi et de débats réguliers. Cela pourrait contribuer à établir une position commune relative à ce qui constitue ou non un comportement acceptable dans le cyberspace, ce qui pourrait aider à prévenir les cyberconflits et à promouvoir la stabilité.

- **Encourager la mise en commun des informations** : le programme d'action devrait encourager les États à mettre en commun des informations sur les cybermenaces et les cyberattaques, notamment des indicateurs de compromission, des échantillons de logiciels malveillants et d'autres informations techniques. Cela pourrait contribuer à mieux apprécier la situation et permettre aux États de réagir plus efficacement aux cyberincidents.
- **Faciliter la coopération et l'inclusion** : le programme d'action devrait faciliter la coopération entre les États, le secteur privé, le monde universitaire et les acteurs non gouvernementaux aux fins du renforcement de la résilience face aux cybermenaces. Il pourrait s'agir d'initiatives visant à promouvoir l'adoption des meilleures pratiques et de normes, les exercices conjoints et les simulations et d'autres formes de collaboration, afin de tirer parti des compétences spécialisées et des ressources de chaque acteur.

En résumé, nous attendons du programme d'action, en tant que future instance de dialogue institutionnel régulier, qu'il constitue une plateforme précieuse permettant aux États d'échanger des bonnes pratiques, de renforcer leurs capacités, d'élaborer des normes et des principes, de mettre en commun des informations et de faciliter la coopération et l'inclusion. Ce faisant, le programme d'action contribuerait à renforcer la résilience des États face aux cybermenaces et à atteindre l'objectif général de maintien de la paix et de la stabilité dans le cyberspace.

Nous réaffirmons la position ferme de l'Albanie en faveur d'un cyberspace mondial, ouvert, libre, stable et sûr, où le droit international, y compris le respect des droits humains et des libertés fondamentales, s'applique pleinement, et d'un développement social, politique et économique.

Nous sommes convaincus de l'importance de l'action multilatérale pour ce qui est de poursuivre le dialogue entre les États Membres et, en ce qui concerne les modalités de mise en place d'un programme d'action, nous entendons poursuivre notre action, en œuvrant avec d'autres États Membres pour renforcer un consensus en faveur de cette proposition et avancer vers la mise en place éventuelle du programme d'action lorsque le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) aura achevé ses travaux en 2025.

Allemagne

[Original : anglais]
[31 mars 2023]

A. Principes fondamentaux du programme d'action

L'Allemagne appuie la mise en place d'un programme d'action qui doterait la Première Commission d'un mécanisme permanent, inclusif et orienté vers l'action permettant l'instauration d'un dialogue institutionnel régulier sur la sécurité et l'utilisation des technologies numériques. Le programme d'action sera l'unique mécanisme de suivi de l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Il deviendra opérationnel après la fin du mandat du groupe et sera chargé de donner suite à ses conclusions.

Il convient d'éviter les mécanismes parallèles ou les doubles structures, car de nombreux États ne seraient pas en mesure d'y participer de manière constructive. Les discussions menées entre les États sur la portée, la structure et la teneur du programme d'action doivent se poursuivre au sein du groupe de travail pour préparer une transition sans heurts. L'objectif doit être de parvenir à un consensus sur le contenu et les modalités du programme d'action, qui devrait être approuvé par tous les États

Membres à l'occasion d'une conférence organisée à cette fin immédiatement après la dernière session du groupe de travail, en 2025.

Le programme d'action a pour objectif général de contribuer à la paix et à la sécurité internationales dans le cyberspace en facilitant le dialogue et la coopération entre les États en ce qui concerne la mise en œuvre du cadre international élaboré pour promouvoir le comportement responsable des États en matière d'utilisation du numérique. Il faut pour ce faire :

- Renforcer les cybercapacités, conformément aux lignes directrices convenues dans le rapport final de 2021 du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, et tirer parti des synergies avec les mécanismes d'autres instances ;
- Adopter des mesures de confiance, notamment en ce qui concerne l'utilisation efficace du futur répertoire mondial d'interlocuteurs ;
- Mettre en commun les meilleures pratiques aux niveaux international, interrégional et régional ;
- Faire participer activement les parties prenantes concernées.

Le programme d'action est en outre appelé à servir de plateforme permanente permettant de faire avancer les questions récurrentes en facilitant le débat sur les menaces existantes et nouvelles et sur la manière dont le droit international, y compris le droit humanitaire international et les droits humains, s'applique à l'utilisation du numérique par les États. Le cadre international de comportement responsable des États dans le cyberspace pourra être adapté dans le cadre du programme d'action pour répondre aux nouvelles menaces à mesure qu'elles évoluent.

Le programme d'action devrait servir de cadre institutionnel global aux autres mécanismes de cybersécurité qui sont en cours d'élaboration au sein du groupe de travail, comme le cyberportail proposé par l'Inde et le cyberregistre suggéré par le Kenya.

L'objectif principal, les objectifs spécifiques et les principes fondamentaux du programme d'action devraient être inscrits dans une déclaration politique qui sera soumise pour adoption à l'Assemblée générale et qu'une résolution de la Première Commission décrivant les fonctions, la structure et les modalités du programme d'action viendra compléter. La déclaration politique et la résolution de la Première Commission se fonderont toutes deux sur les résultats de la conférence dont il est question ci-dessus, qui devrait avoir lieu en 2025.

B. Fonctions, structure et modalités du programme d'action

Les fonctions du programme d'action devraient être définies en s'appuyant sur les enseignements tirés des instruments précédents et existants et en veillant à garantir la participation effective, inclusive et transparente des États. Il faut par ailleurs qu'elles permettent de mesurer les progrès accomplis dans la mise en œuvre du cadre de comportement responsable des États, notamment au moyen d'un mécanisme de compte rendu volontaire comme l'enquête de l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) sur l'application à l'échelle nationale des recommandations de l'ONU en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale. Il faut impérativement renforcer les capacités et encourager la coopération entre les États ainsi qu'avec les organisations régionales et les acteurs non étatiques si l'on veut s'attaquer aux domaines dans lesquels la mise en œuvre au niveau national accuse un retard.

Il est proposé d'adopter la structure et les modalités suivantes :

a) Des conférences annuelles sont organisées au Siège à New York pour :

i) examiner et mesurer les progrès réalisés dans la mise en œuvre du cadre et l'exécution des fonctions ayant été définies ;

ii) discuter de l'évolution potentielle du cadre en veillant notamment à approfondir la compréhension commune de l'application du droit international dans le cyberspace ;

iii) adopter des décisions sur des sujets particuliers ;

iv) mettre en commun des informations sur les menaces actuelles et émergentes contre la paix et la sécurité internationales qui résultent de l'utilisation du numérique ;

v) mettre au point d'autres mesures de renforcement des cybercapacités ;

vi) examiner de quelle façon le programme d'action pourrait être modifié progressivement en tenant compte des besoins des États Membres et de l'évolution des menaces et en partant du principe qu'il s'agit d'un instrument flexible.

b) Des mesures de confiance sont appliquées et améliorées en s'appuyant sur le répertoire mondial d'interlocuteurs qui doit être établi par l'actuel groupe de travail. Le répertoire, qui constitue lui-même une mesure de confiance, sert aussi de fondement à l'application d'autres mesures de confiance, l'objectif général étant de réduire le risque de malentendus et de conflits dans le cyberspace. En facilitant l'application de mesures de confiance spécifiques axées, entre autres, sur la communication, notamment en temps de crise, l'échange entre pairs, la mise en commun des pratiques exemplaires, les mesures de transparence, la coopération avec le secteur privé ou les exercices de simulation conjoints, le répertoire constituerait un pilier central du programme d'action, qui met l'accent sur la mise en œuvre du cadre existant.

c) Le Bureau des affaires de désarmement assure le secrétariat du programme d'action. En plus de préparer les réunions annuelles et les conférences d'examen, le Bureau sera chargé de la gestion du répertoire mondial d'interlocuteurs et d'autres mesures de confiance.

d) L'UNIDIR fournit aux États les instruments de suivi et d'examen dont ils ont besoin (par exemple, des listes de contrôle des normes à appliquer) et mène des activités de recherche liées à la mise en œuvre du cadre.

e) Des réunions supplémentaires des axes de travail techniques pourraient être organisées entre les sessions. Des axes de travail techniques spécialisés pourraient se concentrer, entre autres, sur le renforcement des cybercapacités, les mesures de confiance, l'application du droit international et les menaces actuelles et futures. La participation à ces axes de travail devrait être volontaire et ouverte à tous les États et témoigner d'une représentation régionale équilibrée. Il faudra par ailleurs tenir compte de la capacité des États à participer de manière significative au moment de déterminer le nombre d'axes de travail et leurs modalités de fonctionnement (participation des parties prenantes, fréquence des réunions, etc.). Ces éléments devraient être décidés par consensus lors des réunions annuelles.

f) Des conférences d'examen sont organisées tous les quatre ans de façon que le programme d'action puisse être adapté, si nécessaire, à l'évolution dynamique du cyberspace et aux risques qui en découlent pour la paix et la sécurité internationales.

Les États conserveront le droit exclusif de négocier les textes convenus et de prendre des décisions dans le cadre du programme d'action, certes, mais la collaboration avec les parties prenantes non gouvernementales (organisations multilatérales et régionales, société civile, secteur privé et universités) devrait tout de même être resserrée en offrant des possibilités de participation inclusive et significative inspirées des modalités appliquées par le Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles (un État Membre qui oppose son veto à la participation d'une partie prenante doit justifier publiquement sa position ; l'exclusion d'une partie prenante doit être décidée par un vote). Les parties prenantes ont donc le droit de prendre la parole et de soumettre des contributions écrites lors des réunions annuelles, des conférences d'examen et des réunions supplémentaires des groupes de travail techniques organisées entre les sessions. Le recours à des options de participation hybrides permettrait en outre d'accroître le caractère inclusif des débats.

En ce qui concerne les mesures de confiance et le renforcement des capacités, en particulier, il convient de tirer parti des initiatives et des structures existantes aux niveaux régional et sous-régional ou dans d'autres instances et de créer des synergies (par exemple avec les organisations régionales, le Fonds d'affectation spéciale multidonateur de la Banque mondiale pour la cybersécurité et le Forum mondial sur la cyber expertise).

Les mécanismes de financement qui relèvent d'autres instances des Nations Unies, comme le fonds « Sauver des vies » ou le Mécanisme de financement des Nations Unies pour la coopération en matière de réglementation des armements, qui concernent tous deux la maîtrise des armements, pourraient offrir des orientations utiles sur l'établissement d'un mécanisme destiné à appuyer le renforcement des cybercapacités par la formation et la mise en commun des pratiques exemplaires. En outre, il pourrait être envisagé de créer un programme de bourses permettant à des experts provenant des capitales des pays en développement de représenter leur pays.

On pourrait par ailleurs mettre en place un « système de partenariat » interrégional fonctionnant sur une base volontaire dans le cadre duquel un État disposant de capacités élevées en ce qui concerne la mise en œuvre du cadre serait associé à un ou à plusieurs États ayant des capacités moindres. Un tel mécanisme renforcerait la coopération entre les États, faciliterait le dialogue et la mise en commun de pratiques exemplaires et accroîtrait la capacité des États s'agissant de l'application générale des normes. L'approche de l'Organisation pour la sécurité et la coopération en Europe qui préconise l'adoption de mesures de confiance pourrait servir de modèle de référence à cet égard.

Australie

[Original : anglais]
[12 avril 2023]

En réponse à l'invitation formulée par l'Assemblée générale dans sa résolution [77/37](#), l'Australie se félicite de l'occasion qui lui est donnée de donner son avis sur la portée, la structure et la teneur du programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, ainsi que sur les travaux préparatoires et les modalités de sa mise en place. Notre réponse s'appuie sur l'étude¹ que l'Australie a

¹ Disponible à l'adresse suivante : <https://front.un-arm.org/wp-content/uploads/2020/12/australian-research-paper-revised-december-2020-version-2-owg-regular-institutional-dialogue.pdf>.

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

L'Australie soutient la mise en place, sous les auspices de la Première Commission, d'un mécanisme unique, permanent, flexible, inclusif, transparent et orienté vers l'action, permettant d'examiner, de mettre en œuvre et de faire progresser le cadre de comportement responsable des États dans le cyberspace, convenu et réaffirmé par consensus par l'Assemblée générale, qui consiste en des règles de droit international, des normes et des mesures de confiance et s'appuie sur un renforcement coordonné des capacités. Le programme d'action devrait constituer une instance dans laquelle les 193 États Membres pourraient participer de manière utile, régulière et soutenue aux débats et à la prise de décision. Il devrait pouvoir évoluer, pivoter et se développer – il devrait soutenir la mise en œuvre du cadre convenu existant et donner la possibilité d'en poursuivre le développement, par consensus, au fur et à mesure de l'apparition de nouvelles menaces et de nouveaux défis.

Portée

Les États ont constaté qu'« il était urgent de continuer à renforcer les positions communes, d'instaurer la confiance et d'intensifier la coopération internationale » et ont également 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 » (voir [A/75/816](#)).

Sous les auspices de la Première Commission, le programme d'action devrait porter sur les menaces nouvelles et existantes dans le cyberspace qui pourraient avoir des effets sur la paix, la sécurité et la stabilité internationales ainsi que sur les mesures à prendre pour faire face à ces menaces. L'objectif global du programme d'action devrait être de contribuer au maintien de la paix et de la sécurité internationales en favorisant et en préservant un cyberspace ouvert, sûr, stable, accessible, pacifique et interopérable.

Mandat

Un mandat clair et efficace sera déterminant pour la portée du programme d'action. Ce mandat doit avoir pour socle le cadre convenu et être suffisamment souple pour que, dans le cadre du programme d'action, on puisse s'appuyer sur ce cadre et en poursuivre le développement.

À cet effet, le mandat du programme d'action devrait poser une base claire pour promouvoir, affiner et mettre en œuvre des positions communes et des mesures de coopération afin de faire face aux cybermenaces nouvelles et actuelles dans le contexte de la sécurité internationale, notamment en ce qui concerne la manière dont le droit international s'applique au comportement des États dans le cyberspace, les normes non contraignantes de comportement responsable des États, les mesures visant à instaurer la confiance entre les États et le renforcement ciblé et coordonné des capacités à mettre en œuvre le cadre. Il devrait comporter la possibilité d'évaluer régulièrement s'il est nécessaire de prendre des mesures supplémentaires pour faire face à l'évolution rapide du cyberenvironnement.

Structure et teneur

Déclaration politique

Le programme d'action pourrait être fondé sur une déclaration politique énonçant les engagements des États et prévoyant un mécanisme qui pourrait être

approuvé dans le cadre d'une résolution de l'Assemblée générale. La déclaration politique devrait :

- approuver et réaffirmer l'engagement politique des États à l'égard du cadre (notamment l'application du droit international existant dans le cyberspace), comme convenu dans les rapports successifs du Groupe d'experts gouvernementaux² et dans 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 internationale³.
- rappeler les menaces nouvelles et existantes contre la sécurité internationale liées à l'utilisation malveillante du numérique, en s'appuyant sur les évaluations de la menace présentées dans les rapports du Groupe d'experts gouvernementaux et du Groupe de travail.
- mettre en place un mécanisme institutionnel permanent pour faire progresser la mise en œuvre de ce cadre (notamment en soutenant les capacités des États à cet égard) et les modalités correspondantes.
- donner la possibilité de poursuivre le développement du cadre et de le mettre à jour, le cas échéant, afin d'y inclure des principes, des recommandations et des engagements issus d'un consensus si l'Assemblée générale approuvait par consensus un rapport du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), un rapport du Groupe d'experts gouvernementaux ou d'autres processus des Nations Unies, ou si un accord de consensus était conclu lors d'une conférence d'examen du programme d'action.
- définir les domaines d'action privilégiés du programme d'action, axés sur les questions que la communauté internationale conviendrait de débattre et de traiter.
- promouvoir de façon claire et encourager la concertation avec les membres concernés de la communauté multipartite dans les domaines pertinents.

L'Australie propose que les États affirment leur attachement à une déclaration politique à l'occasion d'une manifestation de haut niveau organisée pendant la première conférence d'examen du programme d'action. La déclaration devrait également pouvoir être mise à jour par consensus et fixer l'ordre du jour de la prochaine série de réunions. En outre, l'Australie a conscience de la place déterminante qu'occupe le groupe de travail dans la mise en place du futur mécanisme et suggère qu'il joue un rôle dans les débats, l'élaboration, les négociations et l'adoption d'une déclaration politique relative au programme d'action et note que toute déclaration politique devrait être acceptée par consensus par tous les pays.

Réunions annuelles, conférence d'examen et réunions techniques

L'Australie demeure souple quant à la fréquence et au type de réunions qui pourraient être convoquées dans le cadre du programme d'action. Par exemple, dans le cadre du programme d'action, on pourrait tenir des sessions formelles annuelles, qui rassembleraient les travaux réalisés dans le cadre des axes de travail techniques organisés durant l'année. Les conférences d'examen pourraient être convoquées à quelques années d'intervalle (par exemple, tous les trois ou quatre ans) pour examiner et mettre à jour la déclaration politique et les engagements et mesures qui en découlent. Les sessions formelles annuelles pourraient juger opportun de créer des

² Voir A/65/201, A/68/98, A/70/174 et A/76/135.

³ A/AC.290/2021/CRP.2.

groupes de travail ou d'établir des axes de travail de manière à se concentrer sur les questions urgentes à faire progresser dans le cadre du programme d'action et elles pourraient adopter des décisions et des recommandations par consensus. Ceci devrait s'appuyer sur les travaux menés dans le cadre des axes de travail techniques, qui devraient être inclusifs, encourager la participation d'experts et se consacrer à telle ou telle question énoncée dans la déclaration politique. Comme point de départ, le premier cycle ou la première session du programme d'action pourrait notamment porter sur des sujets tels que la protection, offerte par le cadre, des infrastructures critiques contre la cyberactivité malveillante, la protection des services de soins de santé et des services médicaux contre la cyberactivité malveillante ou l'application du droit international à des exemples hypothétiques de types de cyberactivité malveillante. À mesure que la technologie progresse, les menaces évoluent et se multiplient, tandis que les difficultés de mise en œuvre demeurent. Par conséquent, le programme d'action devrait servir de moyen d'accroître l'agilité face à ces changements.

En ce qui concerne le règlement de procédure, l'Australie rappelle que le programme d'action devrait exiger un accord de consensus sur toutes les questions (notamment les rapports, les recommandations et les déclarations).

Mise en place

Afin que les activités relatives au programme d'action soient fondées sur des preuves et des données, dans le cadre du programme d'action, on devrait mettre l'accent sur le soutien aux efforts relatifs à sa mise en place, notamment au moyen d'un renforcement des capacités spécifique, ciblé et coordonné. Les mesures de renforcement de telles ou telles capacités devraient être élaborées avec précision dans le cadre du programme d'action. Afin de favoriser un renforcement des capacités ciblé et fondé sur les besoins et des observations factuelles, dans le cadre du programme d'action, on pourrait encourager les États Membres à examiner régulièrement leur mise en œuvre du cadre et à faire rapport d'eux-mêmes (par exemple, tous les trois ans ou en fonction du cycle de la conférence d'examen), en utilisant un mécanisme de communication de l'information standard, à savoir l'enquête sur l'application à l'échelle nationale des recommandations de l'Organisation des Nations Unies en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale (disponible à l'adresse suivante : <https://nationalcybersurvey.cyberpolicyportal.org/>). Nous proposons également que le programme d'action prévoie une consultation régulière des parties prenantes concernées.

Travaux préparatoires et modalités de mise en place

Le groupe de travail joue un rôle clé dans l'élaboration du programme d'action et les travaux préparatoires y relatifs. Le programme d'action devrait s'appuyer sur les avancées consensuelles obtenues de haute lutte et sur la somme des débats des six derniers Groupes d'experts gouvernementaux et des groupes de travail initial et actuel. Un mécanisme permanent constitue la phase suivante ou l'évolution de la cyberarchitecture des Nations Unies, qui s'appuie sur ce qui a été fait auparavant et garantit que ces questions recevront l'attention et auront l'importance qu'elles méritent à l'avenir. Le lancement du programme d'action ne devrait avoir lieu qu'à l'issue des travaux du groupe de travail actuel.

Conclusion

Pour résumer, l'Australie insiste sur le fait que le programme d'action devrait avoir un mandat clair qui s'appuie sur le cadre convenu et le réaffirme ; être souple, à la fois sur le fond, en ce sens que le développement du cadre peut être poursuivi par

consensus, et sur le plan de la procédure ; soutenir l'action menée pour mettre en œuvre le cadre au moyen de la communication volontaire de l'information et du renforcement des capacités ; être inclusif, dans la mesure où les décisions portant sur les questions relatives à la sécurité internationale restent la prérogative des États, tandis que les débats et les groupes de travail sont ouverts à toutes les parties prenantes.

Nous attendons avec intérêt de continuer à travailler avec le Secrétaire général, le Bureau des affaires de désarmement et les États Membres afin d'élaborer un programme d'action efficace, souple et inclusif.

Autriche

[Original : anglais]
[13 avril 2023]

L'Autriche soutient fermement la mise en place d'un programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. Conformément au paragraphe 3 de la résolution [77/37](#) de l'Assemblée générale, l'Autriche souhaite souligner l'importance des points suivants en ce qui concerne la portée, la structure et la teneur du programme d'action :

1. En tant que mécanisme de la Première Commission, le programme d'action devrait porter sur les questions liées à l'utilisation du numérique dans le contexte de la paix et de la sécurité internationales. Son objectif fondamental serait de contribuer au maintien de la paix et de la sécurité internationales en préservant un environnement numérique ouvert, stable, sûr, accessible et pacifique, fondé sur le respect du droit international et des droits humains. Selon l'Autriche, la mise en place d'un programme d'action en tant que mécanisme permanent semble être le moyen le plus approprié pour atteindre cet objectif.
2. Par la fourniture et la mise à jour régulière des ensembles de recommandations pratiques aux fins de l'action menée au niveau national, la mise en œuvre du cadre de comportement responsable des États devrait être au cœur des travaux du programme d'action. À mesure que les technologies se développent, le programme d'action devrait s'attaquer aux nouvelles menaces et aux nouveaux défis qui se présentent en poursuivant le développement du cadre, le cas échéant, ou en aidant les États à adapter leur action aux nouvelles menaces et aux nouveaux défis.
3. L'une des principales priorités du programme d'action devrait être de soutenir les efforts de renforcement des capacités concernant la mise en œuvre du cadre (notamment en cherchant à tirer parti des efforts et initiatives existants) et de renforcer la coopération multipartite dans ce domaine ainsi que la coordination avec d'autres initiatives pertinentes.
4. De plus, le programme d'action devrait faire progresser les débats sur la mise en œuvre de tel ou tel aspect du cadre (une norme ou un sujet précis, par exemple, la création d'une équipe nationale d'intervention informatique d'urgence ou la protection des infrastructures critiques). Des réunions d'information régulières pourraient également être organisées avec d'autres organisations (par exemple, l'Union internationale des télécommunications, le Groupe de la Banque mondiale ou le Fonds d'affectation spéciale multidonateur pour la cybersécurité) afin de tenir compte des activités menées dans le cadre de leurs mandats.
5. Tout en soulignant la responsabilité première des États pour ce qui est de maintenir la paix et la sécurité internationales et le rôle central qu'ils jouent dans la

mise en place du programme d'action, la collaboration avec la société civile, le secteur privé, le monde universitaire et la communauté technique est essentielle pour que les États mettent en œuvre les engagements qu'ils ont pris au titre du cadre. Les modalités des réunions du programme d'action devraient donc permettre à toutes les parties prenantes d'assister aux sessions formelles, de faire des déclarations et d'apporter des contributions, comme c'est le cas dans d'autres processus de la Première Commission pour lesquels leur expertise est utile, tels que la réunion d'experts sur les systèmes d'armes létaux autonomes relevant de la Convention sur certaines armes classiques.

6. L'Autriche souligne qu'il importe que les États fassent preuve d'une volonté politique à l'égard du cadre de comportement responsable des États dans le cyberspace et souligne également que le programme d'action devrait être fondé sur un document politique réaffirmant le cadre normatif énoncé dans les rapports finals de 2021 du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberspace dans le contexte de la sécurité internationale et du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

Belgique

[Original : anglais]
[14 avril 2023]

À la suite de la résolution [77/37](#) de l'Assemblée générale, de la communication ODA/2023-001/Programme d'action ICT security du 14 décembre 2022 et de la prolongation du délai au 14 avril 2023, la Belgique communique ses vues sur un programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale.

La Belgique souhaiterait faire les remarques suivantes :

1. Contexte

Depuis 2003, une série de groupes de travail ont fixé un cadre de comportement responsable des États en matière d'utilisation du numérique (les acquis), qui a été approuvé par l'Assemblée générale dans les résolutions de consensus [70/237](#) et [76/19](#) et réaffirmé dans divers documents, notamment ceux du groupe de travail. La mise en place d'un « dialogue institutionnel régulier » a également été débattue. En ce qui concerne le cadre normatif, il a été noté que ce cadre était cumulatif et évolutif : de nouvelles normes pourraient être élaborées au fil du temps.

La valeur ajoutée d'un programme d'action serait de fournir un mécanisme institutionnel permanent et inclusif pour soutenir et suivre l'application des normes convenues. Il devrait s'agir d'un mécanisme pragmatique.

2. Portée et objectifs

Le programme d'action porterait sur des questions relatives à l'utilisation du numérique dans le contexte de la sécurité internationale (mécanisme de la Première Commission). L'objectif fondamental du programme d'action serait de contribuer au maintien de la paix et de la sécurité internationales et d'un environnement numérique ouvert, stable, sûr, accessible et pacifique. Le programme d'action viserait donc expressément à promouvoir la coopération, la stabilité et la résilience mondiales.

Il devrait reposer sur plusieurs principes clés :

a) Il devrait constituer une structure institutionnelle permanente dans laquelle traiter les questions cybernétiques, qui sont maintenant une question bien établie à la Première Commission ;

b) Il devrait réaffirmer avec clarté que le cadre de comportement responsable des États déjà établi servira de base à ses travaux futurs, par exemple, au moyen d'un document politique fondateur qui rappellerait la pertinence du cadre ;

c) Il devrait être souple afin de permettre la large participation des États et de faire face aux nouveaux défis à mesure qu'ils apparaissent. Par exemple, dans le cadre du programme d'action, on pourrait tenir des réunions plénières annuelles ou semestrielles ouvertes à tous les États, qui prendraient des décisions (par exemple, sur l'application des normes ou la poursuite de leur élaboration) en fonction des travaux réalisés durant l'intersession par les groupes de travail techniques (dont certains pourraient se réunir à New York et d'autres à Genève). Dans le cadre des réunions plénières, on pourrait décider de créer des groupes de travail chargés de s'occuper des questions nouvelles ;

d) Il devrait donner la possibilité d'actualiser le cadre sur la base d'un consensus, par exemple, au moyen de réunions plénières ou de conférences d'examen régulières qui pourraient réexaminer le cadre et décider d'en poursuivre le développement, le cas échéant (les travaux de ces conférences d'examen pourraient être préparés durant l'intersession par des groupes de travail portant sur telle ou telle question et dans le cadre des réunions plénières) ;

e) Il devrait mettre fortement l'accent sur le soutien aux efforts de mise en œuvre, notamment en communiquant régulièrement l'information y relative, ce qui permettrait de recenser les besoins et les défis les plus urgents, de formuler des recommandations pratiques, actualisées continuellement, pour guider les États dans leurs efforts de mise en œuvre, et de soutenir les activités de renforcement des capacités ;

f) Il devrait garantir que le soutien au renforcement de ses capacités se rapporte au mandat de la Première Commission, qu'il est pertinent pour la mise en œuvre du cadre et qu'il tient compte des initiatives existantes dans ce domaine. On pourrait envisager de coordonner le renforcement des capacités avec les activités entreprises en la matière dans d'autres enceintes (telles que l'Union internationale des télécommunications), en gardant à l'esprit la nécessité pour chaque instance d'agir dans le cadre de son propre mandat ;

g) Le programme d'action devrait garantir l'inclusivité, pour les États et pour les parties prenantes. En ce qui concerne les parties prenantes, le programme d'action devrait clairement réaffirmer que les États sont responsables au premier chef des questions de sécurité internationale (et devraient donc conserver le pouvoir de décision), mais ses modalités devraient permettre aux parties prenantes d'assister à des réunions formelles, de faire des déclarations et de soumettre des contributions écrites.

3. Fondement juridique et fonctionnement

a) La structure du Traité sur le commerce des armes, de la Convention sur l'interdiction de l'emploi, du stockage, de la production et du transfert des mines antipersonnel et sur leur destruction, de 1997, et de la Convention sur les armes à sous-munitions pourrait servir de source d'inspiration au cadre institutionnel ;

b) Le programme d'action pourrait être fondé sur un document politique qui réaffirmerait l'engagement politique des États à l'égard du cadre de comportement

responsable des États, tel qu'il est affirmé dans les résolutions et les rapports pertinents ;

c) Ce document créerait un mécanisme institutionnel permanent qui mènerait les activités suivantes :

i) Examiner et faire progresser la mise en œuvre du cadre (notamment en soutenant les capacités des États à cet égard) : le programme d'action encouragerait notamment la communication régulière de l'information à titre volontaire sur les efforts nationaux de mise en œuvre en créant son propre système de communication de l'information ou en promouvant les mécanismes existants (tels que l'enquête sur l'application à l'échelle nationale des recommandations de l'Organisation des Nations Unies en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale de l'Institut des Nations Unies pour la recherche sur le désarmement). La communication de l'information servirait de base au recensement des priorités concernant l'application des normes et à la définition des besoins en termes de renforcement des capacités. Dans le cadre des réunions annuelles du programme d'action, des recommandations pratiques relatives aux efforts de mise en œuvre au niveau national seraient émises. Des groupes de travail pourraient être créés pour soutenir ces efforts ;

ii) Soutenir l'action menée pour renforcer les capacités afin de répondre aux besoins et de faire face aux défis recensés par les États concernant la mise en œuvre du cadre. Le programme d'action devrait également viser à favoriser l'échange des meilleures pratiques et le transfert des compétences spécialisées, le cas échéant. Il devrait rechercher la coopération des parties prenantes dans ce domaine. Il devrait également s'efforcer de tirer parti des efforts et initiatives existants. Un système de classement pourrait être mis en place afin d'approuver les activités conformes aux objectifs. D'autres organisations pourraient être invitées à exposer leurs points de vue (comme l'Union internationale des télécommunications et le Fonds d'affectation spéciale multidonateur de la Banque mondiale pour la cybersécurité) ;

iii) Poursuivre le développement du cadre, le cas échéant, pour faire face aux nouvelles menaces et renforcer encore la sécurité dans le cyberspace. Le développement pourrait se faire dans le cadre de réunions annuelles ou de conférences d'examen du programme d'action, ce qui permettrait d'adopter de nouvelles normes sur la base d'un consensus ;

iv) Favoriser la coopération multipartite dans les domaines pertinents : il a été confirmé que le renforcement de la coopération (le cas échéant) avec la société civile, le secteur privé, le monde universitaire et la communauté technique était fort utile. Le programme d'action devrait également prévoir des modalités permettant à toutes les parties prenantes d'assister à des sessions, de faire des déclarations et de présenter des contributions. La Convention sur certaines armes classiques pourrait servir de modèle. On trouve d'autres exemples dans la Convention sur l'interdiction des mines antipersonnel et la Convention sur les armes à sous-munitions.

La structure organisationnelle serait la suivante :

a) Réunions régulières : elles pourraient être organisées chaque année (ou en fonction de la périodicité optimale). Ces réunions pourraient i) examiner les menaces nouvelles et existantes ; ii) examiner la mise en œuvre des normes, règles et principes ; iii) examiner plus avant de quelle manière le droit international s'applique à l'utilisation du numérique et recenser les lacunes éventuelles ; iv) débattre de l'application des mesures de confiance ; v) recenser les priorités en matière de

renforcement des capacités, compte tenu également de la communication de l'information à titre volontaire ; vi) déterminer d'autres mesures nécessaires et définir le programme de travail des réunions intersessions. Dans le cadre des conférences annuelles, on pourrait décider par consensus de créer des axes de travail techniques, ouverts à tous les États et aux parties prenantes concernées, qui se concentreraient sur tel ou tel point. La participation d'experts techniques et juridiques serait encouragée ;

b) Réunions intersessions : elles permettraient de faire progresser le programme de travail convenu lors des réunions annuelles. Leurs travaux pourraient être structurés en fonction d'axes de travail techniques sur tel ou tel point, conformément aux priorités et aux domaines de travail définis lors des réunions annuelles ;

c) Conférences d'examen : elles pourraient être organisées tous les quatre ans (ou selon une autre périodicité) afin d'examiner si le cadre doit être mis à jour et de poursuivre son développement si nécessaire. Un axe de travail spécifique pourrait être créé pour approfondir les débats sur la manière dont le droit international s'applique à l'utilisation du numérique et évaluer s'il existe des lacunes dans le cadre qui pourraient nécessiter de poursuivre son développement.

4. Préparation et mise en place

a) Préparation : sur la base de la résolution 77/37 de l'Assemblée générale, l'élaboration du programme d'action pourrait être organisée dans le cadre de réunions intersessions et de sessions spéciales du groupe de travail en 2024 et 2025.

b) Mise en place : la résolution 77/37 de l'Assemblée générale mentionne une « conférence internationale » comme une possibilité pour mettre en place le programme d'action (comme cela a été fait, par exemple, pour le Programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous tous ses aspects). Si les États le décident, la conférence internationale pourrait être convoquée en 2025 afin d'adopter le document fondateur du programme d'action, sur la base des travaux préparatoires réalisés dans le cadre groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

c) La conférence internationale devrait prendre des décisions sur la base d'un consensus, au moins sur les questions de fond. Elle devrait prévoir la participation des parties prenantes concernées.

Canada

[Original : anglais]
[14 avril 2023]

Contexte

Ces dernières années, le domaine numérique a montré des tendances négatives qui pourraient se révéler nuisibles pour la sécurité et la stabilité internationales. Au nombre de ces tendances, on compte l'utilisation croissante du numérique à des fins malveillantes.

Il est donc impératif de faire face à ces menaces potentielles en créant une base permanente sur laquelle édifier et maintenir la paix, la sécurité, la coopération et la confiance internationales dans l'environnement numérique, notamment dans le cadre d'un programme d'action relatif aux questions liées au cyberspace.

Un programme d'action peut être un facteur déterminant en tant qu'instance permanente et inclusive dans laquelle les États Membres de l'Organisation des Nations Unies peuvent évoquer expressément et développer plus avant les engagements qu'ils ont pris en vue de promouvoir la paix, de protéger les acquis en matière de comportement responsable et d'éviter les conflits dans le cyberspace. Le soutien du Canada à un programme d'action implique également la poursuite du développement de la transformation des sociétés et des économies et l'élargissement des possibilités de coopération dans l'environnement numérique.

En particulier, le Canada souligne que tout nouveau mécanisme permanent n'a pas vocation à concurrencer ce qui a été fait avant, ni ce qui existe actuellement, mais qu'il représente plutôt la prochaine évolution des débats des Nations Unies sur le cyberspace, s'appuyant sur les débats et les accords conclus jusqu'à présent.

Le Canada rappelle qu'il a appuyé le précédent rapport de consensus de 2021 du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberspace dans le contexte de la sécurité internationale et, en particulier, 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, dans lequel les auteurs recommandaient que les États examinent des propositions visant à faire progresser concrètement les travaux de manière à mettre en œuvre leurs engagements existants.

Le Canada rappelle en outre les aspects de fond du mandat du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), ainsi que la résolution 73/27, dans laquelle l'Assemblée générale saluait les travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (de 2010, 2013 et 2015) et les rapports pertinents auxquels leurs travaux ont abouti, qui guideront la mise en place du programme d'action auquel ils serviront de socle.

Objectifs

La mise en place d'un programme d'action des Nations Unies sur les questions liées au cyberspace en vue de promouvoir un comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale soutiendra ainsi les objectifs des États :

- Permettre la poursuite des travaux de consensus antérieurs du Groupe d'experts gouvernementaux et du Groupe de travail afin d'examiner, de mettre en œuvre et de faire progresser le comportement responsable des États dans le cyberspace et de poursuivre le développement de ces travaux.
- Prévoir la participation réelle des parties prenantes concernées.
- Créer, sous les auspices de la Première Commission, une instance permanente chargée des questions liées au cyberspace, qui n'aura pas besoin d'être réitérée et dans laquelle les États sont responsables au premier chef des questions de sécurité internationale.
- Veiller à ce que l'organe soit largement représentatif, c'est-à-dire qu'il tienne compte des intérêts de tous les États Membres de l'Organisation des Nations Unies.
- Être une instance orientée vers l'action, en ce sens qu'elle est chargée du suivi du comportement responsable des États dans le cyberspace, qu'elle cherche à favoriser le renforcement de la confiance et qu'elle promeut le renforcement des

capacités afin d'améliorer les capacités des États à appliquer les normes de comportement responsable et le droit international.

- Répondre aux besoins des États en matière de sensibilisation politique aux questions de cybersécurité au niveau national, par l'intermédiaire d'une conférence de haut niveau ou d'une déclaration politique.
- Servir d'instance aux débats continus sur l'avenir du cadre et la poursuite de son développement face aux nouvelles technologies et menaces.

Portée et mandat

En tant que mécanisme stable et permanent, le programme d'action offrirait aux États la possibilité de maintenir le cadre existant et de poursuivre son développement pour faire face aux menaces nouvelles et futures.

En ce qui concerne les menaces, le programme d'action pourrait servir de plateforme non seulement pour recenser les menaces potentielles, mais aussi pour convenir de solutions et mettre en place des mesures visant à atténuer ces risques.

Le programme d'action pourrait également s'appuyer sur les travaux en cours qui visent à rendre opérationnel le cadre normatif, par exemple, les 11 normes convenues par le Groupe d'experts gouvernementaux et approuvées par l'Assemblée générale, en se prévalant de l'enquête sur l'application à l'échelle nationale des recommandations de l'Organisation des Nations Unies en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale de l'Institut des Nations Unies pour la recherche sur le désarmement et la liste de contrôle de la mise en œuvre des normes élaborée par Singapour et le Bureau des affaires de désarmement. Par exemple, une priorité pourrait être d'encourager les États à définir, au niveau national, ce qu'ils considèrent comme des infrastructures critiques, ce qui était un domaine d'intérêt dans le précédent rapport de consensus du Groupe d'experts gouvernementaux.

En outre, l'inclusion de toutes les parties prenantes concernées dans un programme d'action pourrait contribuer à faire progresser la mise en œuvre des normes et à soutenir les États en les encourageant ou en les aidant à faire régulièrement rapport d'eux-mêmes. Le programme d'action pourrait s'appuyer sur les enquêtes existantes relatives à la mise en œuvre afin de permettre aux États de mesurer les progrès accomplis, étant donné que la mise en œuvre des normes sera un processus continu.

Si tant est que les normes font partie du cadre international de cybersécurité, il importe également de mieux comprendre de quelle manière le droit international s'applique au cyberspace. En l'absence d'un large consensus sur la manière dont il s'applique ou d'une compréhension suffisante de celle-ci, on peut encourager les États à faire valoir leur position en la matière dans le cadre du programme d'action. Celles-ci peuvent être collectées, diffusées et débattues afin de renforcer la position commune dans ce domaine.

Le programme d'action pourrait s'imposer comme un modèle coopératif et multipartite afin de faciliter la participation des parties prenantes, qui peuvent à leur tour contribuer aux efforts de mise en œuvre aux niveaux national et régional. L'inclusion des parties prenantes concernées dans une instance spécialisée conférerait une légitimité et permettrait de façonner un instrument qui refléterait les réalités vécues et chercherait à lutter contre les menaces réelles.

Dans le cadre du programme d'action, on pourrait ouvrir le dialogue au niveau régional en coopérant avec des organisations régionales afin de promouvoir des initiatives coordonnées. Le Bureau des affaires de désarmement du Secrétariat,

agissant au moyen des ressources existantes et des contributions volontaires, devrait continuer de collaborer avec les organisations régionales compétentes, dont l'Union africaine, l'Union européenne, l'Organisation des États américains, l'Organisation pour la sécurité et la coopération en Europe, le Forum des îles du Pacifique et le Forum régional de l'Association des nations de l'Asie du Sud-Est, pour organiser d'autres séries de consultations. Celles-ci permettraient aux États membres de ces organisations d'échanger leurs points de vue sur les nouvelles menaces, les normes, les meilleures pratiques, l'application du droit international, le renforcement des capacités et les mesures de confiance une fois que le programme d'action aura été établi en 2025 et ensuite.

Le programme d'action servirait de mécanisme permanent pour maintenir et étoffer un répertoire d'interlocuteurs aux niveaux décisionnel et technique. Ce répertoire, auquel le groupe de travail met actuellement la dernière main, pourrait également être élargi pour inclure, sur une base volontaire, les coordonnées d'autres parties prenantes afin de favoriser une gestion des crises plus rapide lorsque se produisent des cyberincidents.

Le programme d'action devrait faire fond sur les investissements existants dans le renforcement des capacités et l'assistance technique, qui sont essentiels pour atteindre les objectifs énumérés ci-dessus ainsi que pour faciliter la coopération entre les États. Il jouerait le rôle de mesure de confiance globale dans le domaine de la sécurité du numérique.

Sur la base des besoins recensés par les États eux-mêmes, le programme d'action ferait office de plateforme pour faire correspondre les besoins en matière de renforcement des capacités et les ressources correspondantes. Un soutien concret au renforcement des capacités aiderait les États à mettre en œuvre les normes, règles et principes convenus. En tant que fonction, le programme d'action pourrait également intégrer des outils existants de manière à permettre aux États et aux parties prenantes de mettre en commun des propositions pertinentes relatives au renforcement des capacités, tels que le Portail des politiques de cybersécurité de l'Institut des Nations Unies pour la recherche sur le désarmement.

En tant que mécanisme orienté vers l'action, le programme d'action pourrait s'associer à l'action menée par le Forum mondial sur la cyber expertise ou l'Institut des Nations Unies pour la recherche sur le désarmement pour renforcer les capacités et en amplifier les effets. Ces efforts collectifs aideraient les pays à définir leurs besoins en matière de renforcement des capacités afin de les satisfaire.

Structure

Comme l'a indiqué le Canada dans sa précédente communication⁴ sur le programme d'action, on peut tirer des enseignements importants de la mise en place d'autres programmes d'action et d'un certain nombre de recommandations sur la manière de faire du programme d'action un processus consultatif et inclusif. Selon le Canada, la mise en place d'un programme d'action des Nations Unies devrait être structurée et développée de la manière décrite ci-dessous.

Il importe de noter que, une fois établi, le programme d'action ne fonctionnera pas comme un traité, mais comme un mécanisme politique – conçu pour fonctionner par consentement unanime – visant à encourager la coopération volontaire en vue de promouvoir le comportement responsable des États dans le cyberspace.

⁴ Disponible à l'adresse suivante : <https://documents.unoda.org/wp-content/uploads/2022/07/OEWG-Portal-Cover-Letter-Submission-Cyber-PoA-Research-paper.pdf>.

Le Bureau des affaires de désarmement peut servir de secrétariat à la conférence internationale et être le secrétariat du programme d'action. En plus de préparer les réunions annuelles et les conférences d'examen, le Bureau serait également chargé de maintenir le répertoire mondial d'interlocuteurs.

Les progrès réalisés dans la mise en œuvre du programme d'action ainsi que ses priorités de travail futures devraient être examinés deux fois par an, de manière à suivre l'évolution dans le cyberspace.

En tant que processus permanent, le programme d'action ne devrait pas se contenter de produire des rapports et des recommandations. Au contraire, il doit montrer des progrès durables et mesurables. Un programme d'action sur les questions liées au cyberspace pourrait combler les lacunes qui existent actuellement en matière d'application du principe de responsabilité entre les normes existantes et les pratiques réelles en renforçant les engagements pris et en mettant en place des mécanismes de communication de l'information ou des mécanismes d'examen ou en tirant parti des mécanismes existants. Il sera essentiel d'encourager l'établissement de rapports en utilisant les informations qu'ils contiennent ou en offrant la possibilité d'en débattre, par exemple, dans le cadre de réunions obligatoires.

Au moins deux réunions thématiques par an devraient être organisées afin de se concentrer sur des domaines permettant d'encourager la collaboration et de faire progresser les questions cybernétiques.

Les groupes de travail dont la création a été proposée pourraient se pencher sur les nouvelles menaces, les normes et les meilleures pratiques, l'application du droit international, le renforcement des capacités et les mesures de confiance.

Les représentantes et représentants participant à ces groupes de travail pourraient se réunir au moins une fois par an pour suivre les progrès qu'ils ont réalisés dans la mise en place du programme d'action et recalibrer leurs efforts le cas échéant. Ces réunions devraient avoir pour objectif l'élaboration d'un document final contenant des conclusions qui, si elles étaient approuvées à l'unanimité, seraient politiquement (mais pas juridiquement) contraignantes pour tous les participants au programme d'action.

Les décisions relatives aux questions de fond devraient être adoptées par consensus.

Propositions relatives aux prochaines étapes

Le rapport du Secrétaire général comportant les recommandations faites à l'Assemblée générale devrait être présenté à l'Assemblée à sa soixante-dix-huitième session pour décision sur la structure et la teneur du programme d'action et les travaux préparatoires à sa mise en place.

Une conférence internationale devrait être convoquée au plus tard en août 2024. Les organisations internationales et régionales concernées, ainsi que les organisations non gouvernementales, les organisations de la société civile, les établissements universitaires, le secteur privé et la communauté technique devraient y participer.

L'objectif de la conférence internationale n'est pas de copier les travaux du groupe de travail. La conférence concentrerait plutôt son action sur les modalités de mise en place et la teneur du programme d'action, notamment sur les dernières touches à apporter à celui-ci et l'adoption d'une déclaration politique. Cette déclaration élaborerait les éléments clés du programme d'action, le programme de travail futur et un ensemble de priorités concernant les travaux du programme d'action, conformément à la portée du programme d'action, comme le demande la résolution [77/37](#) de l'Assemblée générale.

Dans le cadre du programme d'action, on ne commencerait pas à se réunir avant la fin des travaux du groupe de travail pour la période 2021-2025 et on prendrait en compte dans les travaux relatifs au programme d'action le rapport final du groupe de travail, s'il était adopté par consensus. Les sessions qui auront lieu dans le cadre du programme d'action, une fois celui-ci mis en place, tiendront également compte des rapports de consensus publiés sous les cotes [A/65/201](#), [A/68/98](#), [A/70/174](#), [A/75/816](#) et [A/76/135](#), du rapport d'activité annuel de 2023 du groupe de travail et de tout autre rapport d'activité annuel futur.

Modalités

Compte tenu de la nature du domaine de la cybersécurité et de la propriété diffuse de l'infrastructure cyber et des services clés, les parties prenantes auront un rôle important à jouer dans la mise en œuvre d'un programme d'action sur les questions cybernétiques.

En consultation avec le Bureau des affaires de désarmement, une liste de représentantes et de représentants d'autres organisations non gouvernementales, d'organisations de la société civile, d'établissements universitaires et du secteur privé concernés, y compris ceux ayant des compétences dans le domaine de la cybersécurité, sera établie et présentée pour déterminer quelles parties prenantes pourront participer aux sessions préparatoires, à la conférence internationale et aux sessions du programme d'action.

En ce qui concerne les parties prenantes, les modalités du programme d'action devraient s'inspirer des modalités du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, afin de permettre la participation la plus large possible de la société civile, du secteur privé et des autres parties prenantes concernées.

Dans le cadre du programme d'action, on devrait chercher à tenir compte des questions de genre et à être inclusif et, puisqu'il s'agit d'un instrument en devenir, on devrait trouver des moyens de renforcer les démarches centrées sur l'humain en matière de paix et de sécurité internationales dans le cyberspace.

Chili

[Original : anglais]
[14 avril 2023]

Portée

Le programme d'action devrait porter sur les questions relatives à l'utilisation du numérique dans le contexte de la sécurité internationale. Il devrait viser à promouvoir le comportement responsable des États en matière d'utilisation du numérique et à renforcer la sécurité et la stabilité internationales dans le domaine cybernétique au moyen de propositions pratiques et d'un soutien accru aux efforts de renforcement des capacités en la matière.

Il devrait viser en particulier à : a) mettre la coopération au service de la réduction des tensions, de la prévention des conflits et de la promotion de l'utilisation du numérique à des fins pacifiques, par une approche concertée de lutte contre les cybermenaces, ainsi que par un dialogue inclusif entre les États et avec les parties prenantes concernées ; b) promouvoir la stabilité dans le cyberspace en appuyant la mise en œuvre et la poursuite du développement, le cas échéant, du cadre de comportement responsable des États fondé sur le droit international, y compris le droit

international humanitaire et les droits humains, ainsi que sur les normes de comportement responsable des États, les mesures de confiance et le renforcement des capacités.

Il devrait soutenir les activités pertinentes de renforcement des capacités liées à la mise en œuvre du cadre, en tenant compte des initiatives existantes dans ce domaine et en faisant fond sur celles-ci. À cet égard, il devrait inclure les États et les parties prenantes non gouvernementales.

Structure et teneur

Le programme d'action serait fondé sur un document politique qui rappellerait les menaces nouvelles et existantes contre la sécurité internationale liées aux utilisations malveillantes du numérique, en s'appuyant notamment sur les évaluations de la menace figurant dans les rapports du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, et réaffirmerait l'engagement des États à l'égard du cadre de comportement responsable des États, convenu dans les rapports successifs du Groupe d'experts gouvernementaux et le rapport de 2021 du Groupe de travail, le premier rapport d'activité annuel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) ; les conclusions adoptées par consensus par ce groupe de travail viendront compléter ce cadre, qui est cumulatif et évolutif. Le document politique créerait également un mécanisme institutionnel permanent pour promouvoir la mise en œuvre du cadre (notamment en soutenant les capacités des États en la matière), poursuivre le développement du cadre le cas échéant et encourager la coopération multipartite dans les domaines pertinents.

Dans le cadre du programme d'action, on pourrait tenir des réunions formelles annuelles (ainsi que des conférences d'examen), et les groupes de travail techniques pourraient se réunir durant l'intersession (ils seraient inclusifs et permettraient la participation de tous les États qui en font la demande). Les réunions annuelles adopteraient des décisions et des recommandations par consensus, sur la base des travaux menés durant l'intersession par des groupes de travail techniques spécialement chargés de telle ou telle question. Dans le cadre du programme d'action, on encouragerait la communication volontaire de l'information relative aux efforts de mise en œuvre à l'échelle nationale, et les réunions du programme d'action adopteraient et mettraient régulièrement à jour des recommandations pratiques destinées aux efforts de mise en œuvre à l'échelle nationale. Le programme d'action soutiendrait les efforts de renforcement des capacités liées à la mise en œuvre du cadre et viserait à renforcer la coopération multipartite dans ce domaine ainsi que la coordination avec d'autres initiatives pertinentes.

Travaux préparatoires et modalités de mise en place du programme d'action

En ce qui concerne les travaux préparatoires et les modalités de mise en place du programme d'action, des réunions intersessions et des sessions spéciales du groupe de travail devraient être organisées en 2024 et 2025 afin de poursuivre l'élaboration des différents aspects du programme d'action. Une conférence internationale pourrait être convoquée en 2025 ou 2026 pour adopter le document fondateur du programme d'action, sur la base des travaux préparatoires menés notamment dans le cadre du groupe de travail. La conférence devrait prévoir la participation des parties prenantes concernées.

Colombie

[Original : espagnol]

[14 avril 2023]

Je me réfère à la résolution 77/37 de l'Assemblée générale intitulée « Programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale ». À cet égard, et conformément au paragraphe 3 de la résolution susmentionnée, les vues de la Colombie sur la portée, la structure et la teneur du programme d'action sont exposées ci-après.

Portée

Conformément à la résolution 77/37 de l'Assemblée, le programme d'action aurait pour objectif de mettre en place un programme d'action des Nations Unies destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale.

L'adhésion au programme d'action se ferait à titre volontaire et constituerait un engagement politique. Il s'agirait d'un mécanisme :

- a) permanent : il serait établi pour une durée indéterminée, mais assorti de mécanismes d'examen réguliers ;
- b) inclusif : il garantirait la participation de tous les États et de toutes les parties prenantes concernées ;
- c) transparent : il favoriserait l'élaboration et le renforcement des mesures de confiance, ainsi que la possibilité pour les États de rendre compte de l'action qu'ils mènent pour le mettre en œuvre ;
- d) souple : il serait possible de mettre à jour sa teneur et les mesures de mise en œuvre, en tenant compte de la nature changeante du cyberspace, des menaces croissantes et des défis à relever ;
- e) orienté vers l'action : il recenserait et élaborerait des mesures visant à promouvoir un comportement responsable aux niveaux national, régional et mondial.

Teneur

Le programme d'action pourrait rassembler dans un document unique les recommandations du Groupe de travail, ainsi que les travaux antérieurs des groupes d'experts gouvernementaux, lesquels ont fait l'objet d'un consensus et été approuvés dans le cadre de l'ONU.

En ce sens, le programme d'action devrait s'appuyer sur les travaux réalisés antérieurement dans ces instances et en poursuivre le développement, et élaborer des mesures relatives au cadre de comportement responsable des États en matière d'utilisation du numérique (chaque mesure devrait correspondre à une norme de comportement responsable).

La teneur du programme d'action serait fondée sur les thèmes du Groupe de travail à composition non limitée, tels que définis dans la résolution 75/240 de l'Assemblée générale, et sur les dispositions de la résolution 77/37 de l'Assemblée. Il importe tout particulièrement de suivre la mise en œuvre des normes, règles et principes convenus, ainsi que l'élaboration de futurs cadres normatifs, en tenant compte de la nature changeante et évolutive du cyberspace.

De même, il importe que la portée du programme d'action comporte des mesures de renforcement des capacités afin d'aider les États dans l'action qu'ils mènent pour relever les défis nouveaux et existants dans le domaine du numérique. En rappelant que le renforcement des capacités ainsi que l'assistance et la coopération en la matière sont essentiels pour mettre en œuvre les acquis relatifs au comportement responsable des États dans le cyberspace et pour relever les défis recensés. À ces deux égards, le programme d'action devra être suffisamment souple pour intégrer les questions recensées lors de son élaboration.

De même, le programme d'action établirait un mécanisme de suivi pour examiner les réalisations et les défis liés à sa mise en œuvre efficace, qui servirait également de plateforme en vue de partager les meilleures pratiques et les recommandations relatives à sa mise en œuvre au niveau national ou régional. Ce mécanisme jouerait sans aucun doute un rôle clé dans le renforcement des capacités et la coopération en la matière, et devrait être un pilier fondamental du programme d'action.

Structure

En termes de structure, le programme d'action pourrait comporter des mesures aux niveaux national, régional et mondial qui soient cohérentes et bien articulées, la mise en œuvre des dispositions au niveau national étant la plus importante, car elle déterminerait l'efficacité avec laquelle un État pourrait faire respecter les normes de comportement responsable et faire face aux menaces potentielles liées à l'utilisation malveillante du numérique.

En tant que mécanisme de suivi des mesures prises au niveau national et des réalisations et défis liés à leur mise en œuvre, il serait suggéré d'établir des rapports annuels, de préférence sous forme d'enquête, ce qui en faciliterait l'établissement par les États et permettrait de systématiser et d'analyser les informations d'une manière simple, pratique et opportune.

Pour l'élaboration des mesures à intégrer dans le programme d'action aux niveaux national et régional, un diagnostic des besoins en capacités, des offres d'assistance, des défis communs et des bonnes pratiques pourrait être établi, afin que le programme d'action réponde à la multiplicité des réalités des États qui y participeraient.

Le programme d'action pourrait intégrer et donner suite au plan d'action relatif au renforcement des capacités pour la mise en œuvre du répertoire mondial des points de contact, en créant des synergies et en évitant la duplication des efforts.

En ce qui concerne son fonctionnement institutionnel, le programme d'action établirait un mécanisme d'examen et de suivi, dans le cadre duquel les États tiendraient régulièrement des réunions pour examiner le programme d'action et sa mise en œuvre (y compris ses réalisations et ses difficultés) et mettre à jour et ajuster sa teneur le cas échéant.

Dans le cadre du programme d'action, les États Membres pourraient former des groupes de travail techniques, dans lesquels ils débattraient des questions définies dans le programme d'action et des mesures visant à faire progresser sa mise en œuvre. Ainsi l'instrument serait doté d'un dialogue institutionnel constructif, tout en conservant son caractère opérationnel et orienté vers l'action.

La société civile et les diverses parties prenantes concernées pourraient participer aux groupes de travail techniques à titre consultatif, en tirant parti de leurs connaissances inestimables et de leurs différents points de vue sur la question. Le rôle de la société civile serait également fondamental en ce qui concerne le renforcement

des capacités, le recensement des menaces actuelles et potentielles et, bien sûr, la mise en œuvre concrète des normes de comportement responsable en matière d'utilisation du numérique.

Sachant que le programme d'action se fonderait sur les travaux des groupes de travail à composition non limitée, ainsi que sur les rapports du Groupe d'experts gouvernementaux, les sessions du Groupe de travail qui se tiendront jusqu'en 2025 constituent l'espace multilatéral approprié pour progresser dans l'élaboration de la teneur du programme d'action.

Cuba

[Original : espagnol]

[24 mars 2023]

Le développement du numérique a une incidence croissante sur tous les domaines sociétaux.

Des risques importants découlent de l'utilisation malveillante du numérique et des plateformes des médias, notamment des réseaux sociaux et de la radiodiffusion, ceux-ci servant d'outils d'interventionnisme, par la promotion de discours de haine, l'incitation à la violence, la subversion, la déstabilisation, la diffusion d'informations fallacieuses et la déformation de la réalité à des fins politiques, de la prolifération des cyberattaques et de la militarisation croissante du cyberspace.

Nous rejetons l'utilisation du numérique en vue de transformer le cyberspace en un théâtre d'opérations militaires, ainsi que les tentatives visant à justifier, dans ce contexte, des démonstrations de force unilatérales punitives, y compris le recours à des mesures coercitives unilatérales, voire à des opérations militaires.

Dans le domaine de la cybersécurité, notre pays promeut, comme principe fondamental des relations internationales, la coopération conjointe des États pour prévenir et combattre l'utilisation secrète et illégale, par des personnes, des organisations et des États, des systèmes informatiques d'autres nations, et empêcher que le cyberspace ne devienne un théâtre d'opérations militaires.

Il est nécessaire d'adopter sans plus tarder, dans le cadre de l'Assemblée générale des Nations Unies, un instrument international juridiquement contraignant qui complète le droit international applicable, comble les lacunes juridiques importantes en matière de cybersécurité et permette de relever efficacement les défis et menaces croissants auxquels nous faisons face, au moyen de la coopération internationale.

Cependant, nous pensons que la proposition visant à créer un programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, même si elle part d'une bonne intention, aurait, tant qu'elle se concentre uniquement sur des engagements non contraignants, l'effet néfaste d'éloigner encore plus la possibilité d'adopter des obligations juridiquement contraignantes, que Cuba considère comme le seul moyen véritablement efficace de parvenir à un comportement responsable des États dans le cyberspace.

L'examen des propositions faites par les États fait partie du mandat du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Toute initiative en matière de cybersécurité, y compris un programme d'action, doit être examinée dans le cadre du groupe de travail.

Il appartient au groupe de travail de recommander les mesures les plus appropriées pour l'avenir, sur la base du consensus atteint par les États Membres. Nous sommes contre la création de mécanismes parallèles, faisant double emploi ou se substituant au groupe de travail, à moins qu'ils ne résultent de celui-ci.

La proposition visant à mettre en place un programme d'action nécessiterait des débats plus approfondis entre les États dans le cadre du groupe de travail. Il ne faut pas préjuger de l'issue des débats du groupe de travail, ni des recommandations qu'il soumettra à l'Assemblée générale.

Nous soutenons fermement l'objectif visant à garantir un comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, mais nous sommes contre la création de mécanismes parallèles au groupe de travail ou de mécanismes se substituant à celui-ci. Il est de notre responsabilité de faire bon usage des ressources financières limitées dont nous disposons et d'éviter la prolifération de processus et de réunions parallèles, avec les difficultés qui en découlent pour ce qui est d'assurer la participation à ceux-ci, en particulier celle des plus petites délégations des pays en développement.

Le rôle du groupe de travail, qui consiste à engager un dialogue institutionnel régulier dans le domaine de la sécurité et de l'utilisation du numérique, devrait être respecté et préservé. Nous préconisons la poursuite des travaux sous cette forme, afin qu'ils puissent aboutir à des résultats acceptés par tous les États.

En ce qui concerne la portée du programme d'action, les éléments n'ayant pas fait l'objet d'un consensus ne peuvent être inclus, car ceci compromettrait tout résultat futur.

Un éventuel programme d'action doit contenir des mesures concrètes de coopération internationale, ce qui est une priorité pour les pays en développement. Nous sommes contre l'application de mesures coercitives unilatérales, qui entravent l'assistance et la coopération techniques et le transfert de technologies.

Nous appelons l'attention sur la participation des organisations régionales au développement de cette initiative. Tout en prenant en compte la contribution qu'elles peuvent apporter, nous ne pourrions pas accepter des propositions émanant d'organisations régionales exclusives dans lesquelles tous les pays de la région ne sont pas représentés. La nature intergouvernementale du processus doit primer.

Danemark

[Original : anglais]

[13 avril 2023]

Depuis 2003, plusieurs groupes de travail des Nations Unies ont débattu de la mise en place d'un « dialogue institutionnel régulier » sur les questions relatives au numérique et à la sécurité internationale.

Ce dialogue institutionnel devrait être axé sur le soutien à la mise en œuvre du cadre normatif, comme l'a également dit clairement le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui a conclu que le futur dialogue institutionnel 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 »⁵.

⁵ A/75/816, par. 74.

Le programme d'action constituerait un mécanisme permanent et institutionnel de suivi de la mise en œuvre des normes convenues, dispenserait et mettrait régulièrement à jour des recommandations et soutiendrait ou promouvoir des projets de renforcement des capacités pertinents. En même temps, le programme d'action serait souple et permettrait de poursuivre le développement du cadre, le cas échéant.

Le programme d'action porterait sur des questions relatives à l'utilisation du numérique dans le contexte de la sécurité internationale. L'objectif principal du programme d'action serait de contribuer à la paix et à la sécurité internationales en maintenant un environnement numérique ouvert, libre, stable, sûr, accessible et pacifique.

Le programme d'action pourrait avoir pour socle un document politique qui :

- a) réaffirmerait l'attachement des États au cadre de comportement responsable des États ;
- b) créerait un mécanisme institutionnel permanent visant à faire progresser la mise en œuvre du cadre et à favoriser la coopération multipartite, le cas échéant.

Dans le cadre du programme d'action, on pourrait organiser des réunions formelles une fois par an et prévoir la possibilité que les groupes de travail techniques se réunissent durant l'intersession.

Lors des réunions annuelles, on adopterait des décisions et des recommandations par consensus, sur la base des travaux menés durant l'intersession par des groupes de travail techniques spécialement chargés de telle ou telle question.

Dans le cadre du programme d'action, les États rendraient compte à titre volontaire de la mise en œuvre à l'échelle nationale du cadre de comportement responsable des États au moyen de mécanismes nouveaux ou existants afin de recenser les priorités en matière d'application des normes.

Lors des réunions du programme d'action, il serait possible d'adopter et de mettre à jour des recommandations relatives aux efforts de mise en œuvre à l'échelle nationale. Des groupes de travail pourraient être créés en vue de faire progresser la mise en œuvre de tel ou tel aspect du cadre.

Dans le cadre du programme d'action, on appuierait le renforcement des capacités liées à la mise en œuvre du cadre et viserait à améliorer la coopération et la coordination multipartites avec d'autres initiatives pertinentes.

La valeur de la collaboration avec les parties prenantes telles que la société civile, le secteur privé, le monde universitaire et la communauté technique a été soulignée par le Groupe de travail, qui a conclu que les parties prenantes elles-mêmes « avaient la responsabilité d'utiliser les technologies de l'information et des communications d'une manière qui ne mette pas en danger la paix et la sécurité »⁶. Les parties prenantes privées contribuent également aux efforts de renforcement des capacités, et il peut être essentiel pour les États de coopérer avec elles afin de mettre en œuvre les engagements qu'ils ont pris au titre du cadre.

Les modalités des réunions du programme d'action et des groupes de travail devraient donc permettre aux parties prenantes d'assister aux sessions formelles, de faire des déclarations et d'apporter leur précieuse contribution.

En ce qui concerne les travaux préparatoires et la mise en place du programme d'action, des réunions intersessions et des sessions spéciales du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025)

⁶ Ibid., par. 10.

devraient être organisées en 2024 et 2025 afin de poursuivre l'élaboration des différents aspects du programme d'action.

En outre, la résolution 77/37 de l'Assemblée générale prévoit notamment la possibilité d'organiser une conférence internationale pour mettre en place le programme d'action. Une conférence pourrait être convoquée en 2025 ou 2026 pour adopter le document fondateur du programme d'action sur la base des travaux préparatoires réalisés jusqu'à cette date, notamment dans le cadre du groupe de travail. La conférence devrait permettre d'assurer la participation des parties prenantes concernées.

Égypte

[Original : anglais]
[11 avril 2023]

I. Introduction

1. Les États Membres partagent les préoccupations croissantes de la communauté internationale concernant la prolifération des usages malveillants des technologies de l'information et des communications (TIC) et le développement excessif, par un certain nombre d'États, de capacités numériques dont les fins sont incompatibles avec le droit international et les objectifs du maintien de la paix et de la sécurité internationales et qui sont susceptibles de porter atteinte à l'intégrité des infrastructures d'autres États, nuisant ainsi à leur sécurité dans les domaines civil et militaire.

2. L'Organisation des Nations Unies a déjà commencé à répondre à ces préoccupations. Les groupes d'experts gouvernementaux de 2010, 2013, 2015 et 2021 chargés d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale⁷ ont ainsi formulé des constatations et des recommandations qui ont permis d'élaborer, dans ce contexte, un cadre cumulatif et évolutif pour promouvoir le comportement responsable des États en matière d'utilisation du numérique.

3. Les États Membres ont été invités à s'inspirer, pour ce qui touche à l'utilisation du numérique, des rapports de 2010, 2013, 2015 et 2021 des groupes d'experts gouvernementaux et du rapport de 2021 du Groupe de travail. En outre, il est indiqué dans le cadre convenu que le droit international, et en particulier la Charte des Nations Unies, est applicable et essentiel au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement ouvert, sûr, stable, accessible et pacifique pour les TIC.

4. Le cadre existant de normes, règles et principes de comportement responsable des États en matière d'utilisation du numérique peut contribuer à réduire les risques pour la paix, la sécurité et la stabilité internationales sans limiter ou interdire des actes qui respectent le droit international.

5. Le programme d'action proposé vise à faire fond sur les acquis et le cadre déjà approuvé par consensus par l'Assemblée générale.

6. Le programme d'action proposé ne compromet en rien les travaux actuels du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), car sa mise en place aurait lieu après la fin du mandat du

⁷ Voir [A/65/201](#), [A/68/98](#), [A/70/174](#), [A/75/816](#) et [A/76/135](#).

groupe, en 2025. Il permettrait en outre d'éviter les doubles emplois ou la tenue d'activités en parallèle. Sous les auspices de l'Organisation, il servirait de guichet unique pour traiter des questions relatives aux progrès de l'informatique et des télécommunications et à la sécurité internationale et pour promouvoir le comportement responsable des États en matière d'utilisation du numérique. Pour y parvenir, il mettrait l'accent sur le suivi de la mise en œuvre du cadre selon une approche orientée vers l'action.

II. Objectifs et portée du programme d'action

7. Servir de plateforme de dialogue institutionnel régulier permettant à tous les États de participer à un mécanisme permanent, inclusif, transparent, orienté vers l'action et fondé sur les résultats et le consensus. Le mécanisme en question s'appuierait sur le cadre existant en assurant le suivi de la mise en œuvre de ce dernier, en recensant les lacunes, en adaptant les programmes de renforcement des capacités et en promouvant la coopération internationale et la transparence.

8. Constituer, sous les auspices de l'Organisation, une plateforme orientée vers l'action qui vise à :

a) Évaluer périodiquement la mise en œuvre du cadre convenu par les États Membres en examinant les rapports nationaux de mise en œuvre qu'ils ont présentés sur une base volontaire (les États Membres pourraient s'entendre sur un modèle harmonisé de rapport qu'il convient de suivre) ;

b) Recenser les lacunes et les difficultés variées que rencontrent les États Membres dans la mise en œuvre du cadre et promouvoir des recommandations pertinentes et réalisables pour y faire face et ainsi faire progresser la mise en œuvre du cadre convenu. Il peut s'agir de formuler de nouveaux principes, normes et règles ou des obligations juridiquement contraignantes ;

c) Prendre des mesures pratiques pour promouvoir la coopération internationale et déterminer périodiquement si des actions supplémentaires sont nécessaires pour faire face aux difficultés existantes et nouvelles en tenant compte de l'évolution rapide de l'environnement numérique ;

d) Élaborer des orientations concrètes pour aider les États Membres à appliquer les normes, règles et principes convenus ;

e) Mettre en commun des informations sur les pratiques exemplaires qui peuvent être mises en œuvre aux niveaux national, régional et international (dont les cadres législatifs et administratifs et les mesures prises pour protéger les infrastructures critiques) ;

f) Faciliter la communication directe entre les interlocuteurs nationaux au moyen d'un répertoire mondial spécialisé qui pourrait s'appuyer sur la création du répertoire d'interlocuteurs chargés de la sécurité de l'utilisation du numérique ou en bénéficiaire (si les États en décident ainsi) ;

g) Créer un portail à l'intention des États contenant des modules sur la facilitation des communications entre les interlocuteurs nationaux, notamment en ce qui concerne le signalement des faits, l'archivage de documents et la cartographie de l'assistance (proposition de cyberportail présentée par l'Inde). Le portail permettrait en outre, selon qu'il convient, de prendre contact avec les parties prenantes concernées pour qu'elles fassent connaître leurs positions et leurs propositions ;

h) Appuyer concrètement le renforcement des capacités en se fondant sur l'évaluation des besoins de l'État bénéficiaire et en respectant les principes énoncés à ce sujet dans le document [A/76/135](#). Il devrait être envisagé de créer un mécanisme

de financement spécifique au titre du programme d'action en s'appuyant notamment sur des instruments existants ou nouveaux, comme le Fonds d'affectation spéciale multidonateur de la Banque mondiale pour la cybersécurité ;

- i) Prévenir les conflits que l'utilisation du numérique peut engendrer et chercher à régler les différends par des moyens pacifiques ;
- j) Promouvoir l'utilisation pacifique des TIC ;
- k) Assurer la coordination avec d'autres initiatives régionales pertinentes, selon qu'il convient.

III. Mise en place du programme d'action

9. Les vues et les propositions présentées par les États Membres dans le cadre de l'actuel groupe de travail sur la proposition de programme d'action et dans le rapport du Secrétaire général présenté en application de la résolution 77/380 de l'Assemblée générale ainsi que les recommandations pertinentes figurant dans les rapports du groupe de travail devraient servir à définir la portée, la structure et les modalités du programme d'action.

10. Les États devraient continuer de participer activement au groupe de travail créé en application de la résolution 75/240 de l'Assemblée générale afin de produire des rapports de consensus, dont des recommandations sur la mise en place du programme d'action.

11. Le programme d'action devrait être étoffé et mis au point au sein du groupe de travail actuel de manière à éviter les chevauchements ou la création de mécanismes concurrents et à préserver l'esprit consensuel dans le traitement par les entités des Nations Unies des aspects du numérique qui sont liés à la sécurité internationale.

12. Le programme d'action serait établi après la fin du mandat de l'actuel groupe de travail, en 2025, par une résolution consensuelle de l'Assemblée générale fondée sur des consultations et des préparatifs inclusifs et transparents. L'option d'organiser une conférence portant spécifiquement sur la mise en place du programme d'action sera retenue ou non en fonction des vues exprimées par les États Membres et de l'avis du Secrétaire général sur la nécessité d'une telle conférence. Les États Membres peuvent convenir, au sein de l'actuel groupe de travail, de mettre en place le programme d'action, y compris les modalités proposées, au moyen d'une déclaration politique qui pourrait être approuvée par une résolution de l'Assemblée générale.

IV. Structure et modalités possibles

Réunions périodiques

13. Le programme d'action devrait prévoir l'organisation, tous les six ans, d'une conférence d'examen visant à :

- a) Examiner la mise en œuvre du programme d'action et faire les changements qui s'imposent, dresser une liste des actions qu'il convient de mener en priorité au cours des années à venir et adopter le programme de travail des réunions suivantes ;
- b) Déterminer s'il est nécessaire d'élaborer des normes, règles, principes ou obligations contraignantes supplémentaires sur la base du consensus pour mettre à jour le cadre.

14. Le programme d'action devrait prévoir l'organisation de réunions biennales régulières pour exécuter le programme de travail adopté à la conférence d'examen et assurer le suivi de l'application des normes, règles et principes convenus par les États

Membres en examinant les rapports nationaux de mise en œuvre qu'ils soumettent périodiquement.

15. La présidence de chaque session devrait convoquer des réunions consultatives préparatoires avant chaque conférence d'examen ainsi que des réunions biennales de suivi.

16. Dans le cadre du programme d'action, il pourra être décidé par consensus de tenir des réunions intersessions ou de créer des groupes de travail informels chargés de questions connexes précises, dont l'applicabilité du droit international et l'élaboration de nouveaux principes, normes et règles ou d'obligations ou d'instruments juridiquement contraignants, selon qu'il convient.

Rapports

17. Dans le cadre du programme d'action, les États Membres seraient encouragés à présenter sur une base volontaire des rapports nationaux de mise en œuvre, tous les deux ans en alternance, l'objectif étant qu'ils présentent un minimum d'un rapport tous les trois cycles, soit tous les six ans. Ce processus pourrait s'inspirer du modèle d'enquête sur l'application à l'échelle nationale des recommandations de l'Organisation en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale. Les États Membres peuvent également souhaiter inclure dans leurs rapports nationaux de mise en œuvre une section décrivant leurs priorités et leurs besoins en matière de renforcement des capacités.

18. À l'issue de chaque réunion biennale et de chaque conférence d'examen devra être adopté par consensus un rapport final contenant un document qui sera soumis à la prochaine session de la Première Commission pour examen et approbation.

Prise de décisions

19. Dans le cadre du programme d'action, les décisions sur les questions de fond devraient être adoptées par consensus.

Secrétariat

20. Le Bureau des affaires de désarmement devrait assurer le secrétariat du programme d'action.

Participation des parties prenantes

21. Le programme d'action est un processus intergouvernemental dans lequel la négociation et la prise de décisions sont des prérogatives des États Membres.

22. Il est prévu qu'un dialogue de fond, régulier et soutenu soit engagé avec les parties prenantes dans le cadre du programme d'action.

23. Les organisations non gouvernementales compétentes dotées du statut consultatif auprès du Conseil économique et social en application des dispositions de sa résolution 1996/31 feront part au secrétariat de leur intérêt à participer aux travaux du programme d'action.

24. Les autres organisations non gouvernementales compétentes intéressées dotées d'une expérience et de compétences pertinentes eu égard à la portée et à la finalité du programme d'action informeront également le secrétariat de leur intérêt à participer en communiquant des renseignements sur les objectifs qu'elles poursuivent et les programmes et activités qu'elles mettent en œuvre dans les domaines qui sont du ressort du programme d'action. Les organisations sélectionnées seront invitées à

participer aux sessions officielles du programme d'action, en qualité d'observatrices, selon la procédure d'approbation tacite.

25. Les parties prenantes accréditées pourront assister aux réunions officielles du programme d'action, présenter des rapports oraux lors des sessions qui leur seront dédiées et soumettre des contributions écrites. Les États Membres sont encouragés à utiliser la procédure d'approbation tacite de manière judicieuse, en gardant à l'esprit la notion d'inclusivité.

26. Un État Membre qui aurait une réserve à formuler eu égard à une organisation non gouvernementale le fera savoir à la présidence du programme d'action et l'informerá de ses motifs s'il le souhaite. La présidence communiquera toute information reçue à tout État Membre qui en fera la demande.

27. La présidence organisera des réunions consultatives informelles avec les parties prenantes entre les sessions.

28. Le programme d'action peut faciliter la coordination avec les initiatives régionales et sous-régionales pertinentes en les invitant notamment à participer et à présenter des contributions.

El Salvador

[Original : espagnol]
[15 avril 2023]

Introduction

Il est intéressant de constater que la plupart des États Membres des Nations Unies accordent de plus en plus d'importance à ce qui se passe dans le cyberspace, lequel est régi par le droit international et la Charte des Nations Unies et les droits et obligations des États qui y figurent⁸.

La dépendance croissante à l'égard des technologies de l'information et des communications (TIC) et les capacités susceptibles d'être développées dans le cyberspace peuvent avoir une incidence sur les affaires internes d'autres États et perturber gravement la paix et la sécurité.

Il est important que tous les États Membres des Nations Unies comprennent que ce qui se passe dans le cyberspace a des répercussions sur les processus de consolidation et de maintien de la paix et de la sécurité internationales et qu'ils soient donc mieux préparés à relever les défis, à faire face aux problèmes et à tirer parti des occasions qui se présentent.

Puisque la question est à l'étude depuis environ 25 ans au sein de l'Organisation et qu'elle est évolutive et cumulative par nature, il est essentiel que les progrès qui seront réalisés à l'avenir se fondent sur les conclusions adoptées par consensus figurant dans les rapports des groupes d'experts gouvernementaux, du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale⁹ et du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025)¹⁰, sans préjuger des résultats dans le cas du groupe de travail, dont le mandat s'achève en 2025.

⁸ Voir [A/68/98](#), par. 19.

⁹ Voir [A/75/816](#).

¹⁰ Voir la résolution [75/240](#) de l'Assemblée générale ; le mandat court jusqu'en 2025.

Les rapports de 2010, 2013, 2015 et 2021 des groupes d'experts gouvernementaux¹¹ jettent les bases du cadre de normes, règles et principes de comportement responsable des États dans le cyberspace.

L'évolution des débats et de la vision commune des États favorisera un respect accru des normes consensuelles fondées sur des engagements politiques et une transition vers le prochain stade normal de développement du droit, à savoir l'élaboration de normes juridiquement contraignantes régissant le comportement des États dans le cyberspace.

Objectifs et portée

Objectif général

Le programme d'action devra s'imposer en tant que mécanisme régulier orienté vers l'action qui permet de suivre les progrès des technologies de l'information et des communications dans le contexte de la sécurité internationale en préservant un environnement numérique ouvert, stable, sûr, accessible, abordable et pacifique. La prise de décision devrait être consensuelle sur le fond, conformément à la pratique qui s'est développée autour de ce processus.

Objectifs spécifiques

Offrir un cadre institutionnalisé permettant de répondre dans des conditions plus favorables aux besoins urgents de la communauté internationale en matière de coopération internationale et d'aide (dont l'aide financière et technique), l'idée étant d'appuyer et de faciliter les efforts qui sont faits aux niveaux national, régional et international pour faire face aux menaces dans le domaine de la sécurité de l'information.

Faire progresser la vision commune de la mise en œuvre du cadre existant de comportement responsable des États dans le cyberspace, qui porte sur l'applicabilité du droit international, les menaces qui se posent ou qui pourraient se poser, les mesures de confiance dans le cyberspace et le renforcement des capacités.

Créer un environnement propice à la réduction des fractures numériques, en particulier celle qui persiste entre les hommes et les femmes, renforcer la cyberrésilience et maintenir une approche centrée sur l'humain¹².

Structure

Le programme d'action pourrait se fonder sur un document politique approuvé par l'Assemblée générale ayant pour objectif de créer un mécanisme institutionnel permanent. Il faudra prévoir les ressources et l'expertise technique qui seront mises à disposition pour promouvoir la mise en œuvre du programme d'action.

Le Bureau des affaires de désarmement de l'ONU assurera le secrétariat et veillera ainsi au bon fonctionnement de la structure.

Mise en place

Les vues et les propositions présentées par les États Membres, qui figurent dans le rapport du Secrétaire général présenté en application de la résolution 77/37 de l'Assemblée générale¹³, et les conclusions adoptées par consensus par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation

¹¹ Voir [A/65/201](#), [A/68/98](#) et [A/70/174](#) et [A/76/135](#), respectivement.

¹² Voir la résolution 77/37 de l'Assemblée générale.

¹³ Ibid., par. 3.

(2021-2025) devraient servir à définir la portée, la structure et la teneur du programme d'action.

Un engagement actif dans les discussions portant sur le dialogue institutionnel régulier du groupe de travail peut donner lieu à des contributions pertinentes concernant la mise en place du programme d'action, et ce dernier peut être approuvé en tant que recommandation du groupe de travail si un tel consensus est atteint.

S'agissant de ce processus, il faut éviter de dupliquer les initiatives en cours.

En outre, l'organisation de vastes consultations informelles peut offrir aux États Membres une autre tribune pour exprimer leurs idées, leurs priorités et leurs intérêts en ce qui concerne la mise en place du programme d'action et ainsi permettre à ceux qui ne présentent pas de position nationale d'apporter une contribution supplémentaire.

La mise en place du programme d'action sera facilitée par la désignation d'interlocuteurs chargés d'assurer la liaison entre les États sur les questions de mise en œuvre. Selon qu'il convient, on pourra envisager des synergies avec l'initiative relative au répertoire mondial d'interlocuteurs, qui s'inscrit dans le cadre des mesures de confiance adoptées par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), une fois que les modalités de mise en œuvre auront été définies.

On peut envisager la possibilité d'organiser une conférence internationale quatre ans après la mise en place du programme d'action pour examiner les progrès réalisés à cet égard.

Des réunions des États parties seront organisées deux fois par an pour examiner la mise en œuvre du programme d'action aux niveaux national, régional et international. L'accent devrait cependant être mis sur l'examen de l'application de mesures concrètes, l'objectif étant d'éviter que des instruments récurrents ayant une finalité déclarative soient négociés à nouveau. Le programme d'action devra être orienté vers l'action et axé sur le renforcement des capacités.

Il pourrait être envisagé de créer des groupes de travail chargés d'examiner entre les sessions les progrès réalisés dans des domaines précis.

La mise en place de programmes de sensibilisation continue à la cybersécurité peut être considérée comme un objectif transversal du programme d'action.

Fréquence des réunions

Pour progresser dans la mise en œuvre du programme d'action et s'assurer du respect de ses grandes orientations, il est jugé opportun :

- d'organiser tous les deux ans des réunions d'examen entre les États parties en adoptant une approche pragmatique ;
- d'organiser tous les quatre ans des conférences d'examen (en attendant les résultats de la première conférence d'examen).

L'idée est de laisser aux délégations suffisamment de temps pour se préparer entre les sessions et de ne pas créer de surcharge de travail en faisant double emploi avec les autres mécanismes existants dans le domaine de la sécurité internationale. Une analyse plus approfondie devra être effectuée pour déterminer les années qui conviendraient le mieux pour commencer le cycle de réunions, l'objectif étant de ne pas les faire coïncider avec celles d'autres mécanismes mandatés dans le domaine du désarmement et de la sécurité internationale.

L'objectif principal des réunions de suivi devrait être de mettre à jour les mesures concrètes relatives à la mise en œuvre des orientations du programme d'action à l'échelle nationale et régionale, selon qu'il convient.

Rapports présentés dans le cadre du programme d'action

Dans le cadre du programme d'action, les États Membres seront encouragés à soumettre des rapports sur une base volontaire. Ceux-ci pourront s'appuyer sur des mécanismes existants, comme l'enquête de l'Institut des Nations Unies pour la recherche sur le désarmement sur l'application des normes de comportement responsable des États dans le cyberspace.

Au moment de concevoir des outils supplémentaires de communication de l'information, il faudra veiller à éviter la lassitude liée à l'établissement de multiples rapports et à rechercher des complémentarités avec les outils existants.

Les nouveaux outils de communication de l'information qui pourraient être adoptés par consensus devront être conviviaux et accessibles en ligne, de sorte que toutes les délégations puissent établir des rapports permettant d'évaluer la mise en œuvre des objectifs du programme d'action et de répondre aux besoins émergents dans le domaine du numérique.

Participation d'autres acteurs intéressés

Les États sont responsables au premier chef du maintien de la paix et de la sécurité internationales, et c'est pourquoi le processus de négociation doit conserver sa nature intergouvernementale.

Toutefois, en raison de la nature privée de l'infrastructure de l'Internet et du rôle joué par d'autres organisations compétentes dans la conception et l'amélioration des technologies, il apparaît essentiel de faire participer la société civile, les organisations non gouvernementales, le monde universitaire et l'industrie. Un mécanisme clair tenant compte des vues de l'ensemble des États Membres sur les modalités de participation des autres parties prenantes sera défini dans le programme d'action adopté par consensus.

Équateur

[Original : espagnol]
[14 avril 2023]

L'Équateur apprécie et soutient les recommandations et les conclusions des groupes d'experts et des groupes de travail, telles qu'elles sont reflétées dans les résolutions de l'Assemblée générale des Nations Unies sur les progrès et l'utilisation du numérique dans le contexte de la sécurité internationale.

L'Équateur considère qu'un dialogue institutionnel régulier devrait être établi pour traiter les questions relatives à l'utilisation du numérique dans le contexte de la sécurité internationale. Ce dialogue devrait être orienté vers l'action, inclusif, transparent, axé sur les résultats et fondé sur les débats antérieurs des groupes d'experts et des groupes de travail concernés.

Dans ce contexte, l'Équateur considère que la mise en place d'un programme d'action constituerait un mécanisme permanent et institutionnel permettant de suivre la mise en œuvre des normes volontaires existantes, par l'élaboration et la mise à jour régulière de recommandations applicables sur le comportement responsable des États, par la promotion des projets de coopération internationale pertinents, des mesures de renforcement des capacités et des mesures de confiance, et par l'analyse de

l'élaboration de nouvelles normes et d'un éventuel instrument juridiquement contraignant en la matière, le cas échéant.

De même, l'Équateur considère que le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) peut être la principale instance dans laquelle poursuivre l'analyse et le développement du programme d'action en vue de sa future mise en place.

Au moyen de la mise en place du programme d'action, nous cherchons à contribuer au maintien de la paix et de la sécurité internationales, en préservant un environnement du numérique ouvert, stable, sûr, accessible et pacifique, qui permette de combler le fossé numérique et le fossé entre les hommes et les femmes, et de prendre des mesures face aux menaces et aux défis nouveaux dans le cyberspace, par le dialogue et le consensus entre les États, ainsi qu'avec les parties prenantes concernées.

L'Équateur est fermement convaincu que c'est aux États qu'il incombe au premier chef de maintenir la paix et la sécurité internationales et qu'ils doivent donc conserver le rôle principal dans le programme d'action, à savoir la prise de décisions et la négociation des documents finals. Toutefois, il apprécie et encourage la participation et la contribution, s'il y a lieu, de la société civile, du secteur privé, du monde universitaire et de la communauté technique à ces délibérations, car ils jouent un rôle clé dans l'utilisation du numérique d'une manière qui ne met pas en péril la paix et la sécurité internationales.

En tant que mécanisme de suivi, le programme d'action devrait faire l'objet d'un examen constant dans le cadre d'une réunion annuelle, au cours de laquelle, dans le même ordre d'idée, de nouveaux groupes de travail techniques pourraient être créés pour traiter les questions ou priorités nouvelles.

Nous sommes conscients du chemin parcouru depuis l'établissement des normes de comportement responsable, grâce auxquelles nous ne partons pas de zéro. En même temps, nous ne considérons pas le programme d'action comme une fin en soi, mais comme un jalon qui nous permettra de continuer d'avancer vers une architecture internationale de la cybersécurité plus solide.

Estonie

[Original : anglais]
[14 avril 2023]

En application des dispositions de la résolution 77/37 de l'Assemblée générale, l'Estonie souhaite présenter une position nationale sur le programme d'action.

Au cours des dernières années, les menaces que représente l'utilisation des technologies de l'information et des communications (TIC) pour la sécurité internationale n'ont cessé de s'intensifier et d'évoluer, le contexte géopolitique actuel étant particulièrement complexe. Les menaces croissantes associées à l'utilisation des TIC ont des effets négatifs sur le développement économique et social, ce qui entraîne des problèmes, et elles ont aussi des répercussions sur la stabilité nationale et internationale. Ces répercussions sont toujours au cœur des discussions multilatérales, comme en témoignent les travaux du Groupe d'experts gouvernementaux et ceux du groupe de travail. L'Estonie aimerait faire part des observations suivantes au sujet de l'instauration d'un dialogue institutionnel régulier dans le cadre du programme d'action. Nous croyons que le programme d'action constituerait un instrument utile pour poursuivre les discussions visant à promouvoir le comportement responsable des États en matière d'utilisation du numérique et qu'il

contribuerait à réduire les tensions, à prévenir les conflits et à favoriser l'utilisation pacifique de ces technologies.

1. Le programme d'action devrait se fonder sur les acquis et sur le cadre de comportement responsable des États, en mettant l'accent sur l'utilisation des technologies numériques par les États dans le contexte de la paix et de la sécurité internationales. L'Estonie estime que les TIC doivent être utilisées d'une manière qui est compatible avec les objectifs de maintien de la stabilité et de la sécurité internationales et qui respecte les acquis dont il a été convenu et le cadre de comportement responsable des États. Nous insistons sur le fait que les États Membres doivent s'inspirer, pour ce qui touche à l'utilisation du numérique, des rapports de 2010, 2013, 2015 et 2021 du Groupe d'experts gouvernementaux, ainsi que du rapport de 2021 du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Le mécanisme du programme d'action devrait se fonder sur ces prémisses et chercher à préserver un environnement numérique ouvert, stable, sûr, accessible et pacifique. L'Estonie estime que plusieurs des initiatives existantes et de celles qu'il est proposé de mettre en œuvre, comme le répertoire mondial d'interlocuteurs, contribueraient au bon fonctionnement du mécanisme du programme d'action.

2. Le programme d'action devrait constituer un mécanisme neutre permettant d'assurer la stabilité institutionnelle. Les petits États doivent avoir une vision claire des processus qui seront mis en place en lien avec les discussions sur l'utilisation du numérique par les États et pouvoir assurer une certaine stabilité institutionnelle à cet égard. L'Estonie préconise donc qu'une structure permanente unique soit mise en place après la fin du mandat de l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) pour poursuivre les discussions sur le sujet. Elle est favorable à la poursuite des discussions sur la structure, les modalités et le calendrier de mise en place du programme d'action en tant que mécanisme visant à promouvoir le comportement responsable des États en matière d'utilisation du numérique en tenant compte des vues de l'ensemble des États Membres. L'Estonie est aussi favorable à l'organisation d'une conférence internationale consacrée à la mise en place du programme d'action, comme il est proposé dans la résolution [77/37](#) de l'Assemblée générale. Elle aimerait également souligner que le mécanisme du programme d'action devrait être fondé sur le principe du consensus. L'Estonie croit qu'avec le programme d'action proposé, l'Assemblée générale n'aura plus à envisager la création de nouveaux cyberprocessus tous les deux, trois ou quatre ans. Elle espère que le programme d'action sera considéré comme un cadre utile et neutre par les États Membres et qu'il ne sera pas nécessaire de mettre en place des mécanismes parallèles.

3. Le programme d'action devrait offrir un cadre général permettant de faire avancer de manière inclusive les différents sujets proposés par le groupe de travail. L'Estonie se félicite de l'intérêt croissant des États Membres s'agissant d'apporter une contribution aux différents sujets abordés dans le cadre des sessions du groupe de travail. Les discussions de l'actuel groupe de travail ont été constructives et se sont appuyées sur une série d'idées proposées par différents États Membres. Nous croyons que le programme d'action pourrait offrir aux États Membres une plateforme pour aborder les questions relatives aux TIC et à la paix et à la sécurité internationales. Il pourrait ainsi servir de cadre général pour présenter et approfondir ces idées. Le programme d'action devrait également prévoir des modalités claires et transparentes en ce qui concerne la participation active des multiples parties prenantes, l'objectif étant de mieux tirer parti de leur expertise et de leurs connaissances.

4. **Le mécanisme du programme d'action devrait permettre la tenue de discussions ciblées.** L'Estonie croit que les divers éléments du programme d'action pourraient être fondés sur les débats ciblés tenus, par exemple, dans le cadre de groupes de travail ouverts à tous les participants intéressés et portant sur divers sujets, y compris, entre autres, les menaces, le renforcement des capacités, le renforcement de la confiance, les normes et le droit international. Une autre possibilité serait que ces groupes de travail se concentrent sur des thèmes plus précis, comme la protection des infrastructures critiques. Alors que les États Membres sont de plus en plus nombreux à exprimer leur point de vue et que les menaces évoluent, le programme d'action offrirait un instrument qui, bien que plus flexible, resterait axé sur l'essentiel et permettrait de poursuivre ces discussions. Nous aimerions aussi souligner qu'il faudrait prendre en compte les capacités limitées des petits États dans la conception du programme d'action et fixer des attentes raisonnables concernant la charge de travail prévue. À cet égard, nous sommes favorables à l'idée d'organiser des conférences annuelles traitant de manière générale de l'utilisation du numérique par les États et de créer des groupes de travail spécialement chargés d'examiner certains sujets.

5. **Le programme d'action devrait offrir un cadre inclusif pour les discussions sur le droit international.** L'Estonie se félicite de la tenue de débats plus animés et plus approfondis sur le droit international et la manière dont il s'applique à l'utilisation du numérique par les États. Le droit international est en pleine évolution et les États Membres gagneraient à développer une meilleure compréhension de la manière dont les règles existantes s'appliquent, à partager leurs points de vue sur le sujet et à analyser plus en détail les éventuelles lacunes. Le programme d'action pourrait offrir un cadre inclusif pour la poursuite de ces discussions.

6. **Le programme d'action devrait être orienté vers l'action et axé sur le renforcement des capacités.** La mise en œuvre du cadre de comportement responsable des États dont il a été convenu devrait être au cœur des discussions futures. Cette démarche peut s'appuyer sur une analyse pratique et transparente de l'état de la situation ainsi que sur la réponse aux besoins et aux demandes concernant le renforcement des capacités. On devrait ainsi, dans le cadre du programme d'action, faire le point sur les initiatives existantes en matière de renforcement des capacités en veillant à ce qu'elles soient bien coordonnées et qu'elles se complètent. On devrait par exemple tenir compte, dans la conception du programme d'action, des ressources et des états des lieux existants, comme le portail Cybil et l'outil CyberNet, qui recense les projets de renforcement des cybercapacités des États membres de l'Union européenne.

États-Unis d'Amérique

[Original : anglais]
[14 avril 2023]

Introduction

Les États Membres de l'ONU ont pris conscience du fait que les technologies de l'information et des communications pouvaient être utilisées à des fins incompatibles avec l'objectif du maintien de la paix et de la sécurité internationales. Pendant de nombreuses années, les États se sont réunis sous les auspices de l'Organisation afin de discuter de ce problème et de tenter d'y remédier. En approuvant par consensus les rapports du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, ils se sont unis autour d'un cadre de comportement responsable des États en matière d'utilisation du

numérique. Axé sur la stabilité internationale, ce cadre se compose du droit international en la matière, y compris la Charte des Nations Unies, d'un ensemble de normes non contraignantes et de mesures de confiance.

Si le cadre a reçu un soutien mondial, sa réussite dépend de l'adhésion des États à ses composantes et de leur mise en œuvre. Comme exprimé en 2015 dans le rapport de consensus du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, les États ont déjà affirmé qu'il était nécessaire d'instaurer un dialogue institutionnel régulier à large participation sous les auspices de l'ONU¹⁴. S'appuyant sur cette position, le Groupe de travail a répété par la suite que les États devaient s'efforcer de créer un mécanisme favorisant le dialogue institutionnel¹⁵.

Dans son rapport de consensus de 2021, le Groupe de travail recommande que ce futur instrument des Nations Unies consacré aux questions numériques soit inclusif, transparent, fondé sur le consensus et axé sur les résultats. C'est le cas du programme d'action : il donne l'occasion aux États de créer un instrument à la fois permanent et flexible qui fera progresser le cadre afin d'améliorer la paix et la sécurité dans le cyberspace et de prévenir les conflits et les dommages causés aux civils par certaines utilisations du numérique. Le programme d'action devrait aussi être le mécanisme permanent et orienté vers l'action qui permettra aux États Membres d'appliquer et de promouvoir le cadre consensuel.

Portée du programme d'action

Dans sa résolution 77/37, l'Assemblée générale a rappelé les constatations et les recommandations formulées par les groupes d'experts gouvernementaux de 2010, 2013, 2015 et 2021, celles du Groupe de travail de 2021 et le premier rapport d'activité annuel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), en particulier le cadre cumulatif et évolutif élaboré pour promouvoir le comportement responsable des États en matière d'utilisation du numérique, et a demandé aux États Membres de s'inspirer de ces rapports et du cadre¹⁶. Soutenu par ces rapports, le cadre est à la base du programme d'action.

Les États Membres devraient définir l'orientation du programme d'action et le modifier ultérieurement en accordant toujours la priorité aux questions pratiques de mise en œuvre et de renforcement des capacités d'application du cadre. Le caractère permanent du programme d'action en fait un solide appui pour les États à cet égard.

Instrument permanent, le programme d'action devrait toutefois être assez flexible pour s'adapter aux menaces futures et pour prendre en compte les besoins des États et leurs pratiques exemplaires en la matière. Le programme d'action doit également permettre aux États de réfléchir à l'opportunité et aux moyens de faire évoluer le cadre.

Les parties prenantes non étatiques devraient faire partie intégrante du dispositif. Le programme d'action doit prévoir des modalités de participation aussi inclusives que possible pour bénéficier des compétences de ces acteurs.

Mise en place du programme d'action

En élaborant le futur programme d'action et en en définissant la teneur, les États devraient avant tout s'efforcer de façonner un dispositif qui facilite l'exécution du

¹⁴ Voir A/70/174, par. 18.

¹⁵ Voir A/75/816, par. 70 à 74.

¹⁶ Voir les dixième et onzième alinéas du préambule de la résolution 77/37 de l'Assemblée générale.

cadre consensuel à l'échelle nationale, qui promeut la coopération entre eux sur les questions de sécurité du numérique et qui permet au cadre d'évoluer en même temps que le consensus.

Pour une efficacité optimale, le programme d'action devrait être lancé à l'occasion d'une conférence internationale¹⁷ qui se tiendrait en 2025, à expiration du mandat du groupe de travail. Les documents finaux de cette conférence, parmi lesquels pourrait figurer une déclaration politique, devraient constituer la base concrète du programme d'action et définir les modalités et règles de fonctionnement de cet instrument. Les réunions ordinaires débuteraient en 2026.

Le mandat proposé pour le programme d'action ayant trait à la paix et à la sécurité en lien avec l'utilisation du numérique, il devrait être exécuté sous l'égide de la Première Commission. Le Bureau des affaires de désarmement pourrait servir de secrétariat logistique. Le programme d'action devrait être exécuté dans la limite des ressources budgétaires existantes, autant que faire se peut.

Structure

Le programme d'action devrait prévoir que les États se réunissent annuellement pour définir les thèmes et les problématiques abordés par les groupes de travail techniques et informels qui seraient convoqués à une fréquence fixée lors de la réunion annuelle ou dans les documents finaux de la conférence. Le contenu des enquêtes menées au niveau national pourrait faire l'objet d'une présentation de la part du Bureau ou de l'Institut des Nations Unies pour la recherche sur le désarmement. Ces réunions donneraient l'occasion aux États d'échanger leurs vues sur les sujets suivants :

- Les retours d'expérience et les pratiques exemplaires des pays concernant l'exécution du cadre ;
- Le renforcement des capacités (besoins et ressources) ;
- Les difficultés et les menaces nouvelles et les moyens d'y remédier dans le cadre du programme d'action.

Outre la réunion annuelle et les réunions régulières des groupes techniques et groupes de travail, le programme pourrait prévoir que se tienne, tous les trois ou quatre ans, une conférence d'examen lors de laquelle les décisions seraient réaffirmées et où l'on débattrait de la nécessité de modifier la teneur ou la structure du programme d'action. Cet examen régulier des documents fondateurs offrirait aux États la flexibilité leur permettant d'adapter le programme d'action en fonction de l'évolution de la situation.

Le programme d'action serait lancé en 2026, dans le prolongement de la conférence de 2025. Puis, chaque année, par une résolution ou une décision, la Première Commission entérinerait les décisions consensuelles prises lors des réunions annuelles, y compris les recommandations concernant la date et le lieu des réunions ultérieures. Elle ferait de même avec les décisions des conférences d'examen, le cas échéant.

Renforcement des capacités

Les pays se trouvant à divers stades de développement de leurs moyens et compétences numériques, les Nations Unies ont compris que le renforcement des capacités était indispensable à la coopération et à la confiance dans le domaine de

¹⁷ Voir la résolution [77/37](#) de l'Assemblée générale, par. 3.

l'informatique et des communications¹⁸. L'ONU a un rôle clef à jouer dans la coordination et la mise en avant des multiples parties prenantes qui travaillent activement au renforcement des capacités numériques et au déploiement des programmes tels que ceux dirigés par les États Membres.

En matière de renforcement des capacités, le programme d'action devrait avant tout être directement lié aux mesures prises par les États au niveau national pour appliquer le cadre. Il devrait aussi faciliter les discussions portant sur les besoins spécifiques des États, ce qui lui permettrait de mieux y répondre. En d'autres termes, son but serait de sensibiliser la communauté internationale sur l'importance du renforcement des capacités numériques en lien avec l'application du cadre et de proposer des orientations et des pratiques exemplaires que les États suivraient au niveau national.

Les États-Unis constatent que nombre d'États méconnaissent encore la nature et l'importance du cadre. Beaucoup manquent aussi des capacités nationales de base en matière de cybersécurité, qui sont pourtant nécessaires pour commencer à appliquer le cadre, notamment les normes et les mesures de confiance. Il existe un ensemble d'entités des Nations Unies et d'entités extérieures à l'Organisation qui possèdent un savoir-faire dans des domaines comme les politiques et stratégies nationales de cybersécurité, la gestion des cyberincidents et la protection des infrastructures critiques, les lois sur la cybercriminalité, la culture et les normes en matière de cybersécurité. Le programme d'action ne devrait ni faire double emploi avec leurs activités ni les remplacer. Toutes contribuent aux politiques nationales de sécurité et, en définitive, à la mise en place du cadre, bien qu'elles ne relèvent pas du mandat du programme d'action.

Participation multipartite

Seuls les États devraient être autorisés à prendre des décisions liées au programme d'action. Toutefois, les parties prenantes non étatiques, telles que la société civile, les milieux universitaires et le secteur privé, jouent un rôle constructif lors des forums multilatéraux en ce qu'ils enrichissent les débats de leur savoir-faire et concourent au renforcement des capacités. Ces acteurs devraient donc pouvoir participer activement aux activités liées au programme d'action en tant qu'observateurs, sans droit de vote.

Pour que le programme d'action inclue au mieux les parties intéressées, il convient de fixer des règles transparentes, basées sur des modèles de référence. Par exemple, on pourrait s'inspirer du règlement du Groupe de travail à composition non limitée sur le vieillissement : les États Membres peuvent contester la participation d'une organisation, mais la décision finale est soumise au vote ; les organisations dont la participation n'a soulevé aucune objection au premier tour d'examen sont autorisées à participer à la séance officielle¹⁹.

Concernant la participation aux séances officielles, on pourrait prendre pour modèle le Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Conformément à son règlement, les diverses parties prenantes peuvent notamment :

- Assister aux séances formelles ouvertes ;
- Faire des déclarations orales sur chaque question de fond inscrite à l'ordre du jour, après les débats des États Membres, si le temps prévu le permet ; le temps

¹⁸ Ibid., vingtième alinéa.

¹⁹ Comme exprimé à la section F du document [A/AC.278/2011/2](#).

disponible pendant les réunions étant limité, elles peuvent désigner des porte-parole, d'une manière juste et transparente, en respectant une répartition géographique équitable, la parité des genres et la diversité des parties prenantes participantes ;

- Présenter des documents écrits dans la limite du nombre de mots fixé, qui sont publiés, dans leur langue originale, sur le site Web du Comité spécial²⁰.

Le programme d'action devrait aussi prévoir des moyens de tirer parti des connaissances existantes et des travaux en cours au niveau régional. En permettant à des entités telles que les parties prenantes de participer aux discussions autour du programme d'action, on favoriserait, dans les travaux menés au niveau de l'ONU, une meilleure prise en compte des efforts, des difficultés et des problématiques spécifiques aux régions.

Travail préparatoire

Les États-Unis ont conscience que la mise en place du programme d'action exigera des efforts significatifs de la part des États Membres. Il conviendrait de poursuivre les discussions sur le programme d'action, y compris au sein du groupe de travail actuel, de sorte que le lancement du programme suive sans heurts la fin des activités du groupe en 2025.

Fédération de Russie

[Original : russe]
[12 avril 2023]

Conformément au paragraphe 3 de la résolution [77/37](#) de l'Assemblée générale, la Fédération de Russie présente ses vues concernant le programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale.

Sur les questions de sécurité internationale de l'information, le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) est le premier et unique mécanisme de négociation inclusif, ouvert, transparent et réellement démocratique de l'ONU. Le principe du consensus permet à tous les États, sans exception, de participer à la prise de décision. Au cours de ses travaux, le groupe de travail a fait la preuve de son efficacité et de sa pertinence.

Il importe de faire évoluer le processus de négociation en s'appuyant sur l'expérience du groupe de travail. À ce sujet, le détail des propositions de la Fédération de Russie figure dans le document de réflexion relatif au dialogue institutionnel régulier (présenté à la quatrième session du groupe, tenue à New York du 6 au 10 mars 2023).

Le programme d'action ne doit pas dicter la décision qui sera prise concernant le mécanisme de négociation de l'ONU relatif à la sécurité internationale de l'information. Au même titre que les propositions soumises par les autres pays, cette initiative doit être débattue au groupe de travail, conformément au mandat de celui-ci, tel que défini dans la résolution [75/240](#) de l'Assemblée générale. Le délai de trois ans (jusqu'en 2025) suffit pour définir conjointement le format qui remplacera le groupe de travail actuel.

Le contenu du programme d'action demeure peu élaboré, et ses objectifs ne sont pas clairs. Les discussions qui se tiennent au groupe de travail montrent que même

²⁰ Voir [A/AC.291/6](#), par. 3.

les partisans du programme n'ont pas de position commune sur ses grands principes, et notamment sur le mode de prise de décision.

En l'état actuel des choses, cette initiative ne peut prétendre au statut de mécanisme de négociation de l'ONU indépendant et inclusif sur la sécurité internationale de l'information. Elle ne présente aucune valeur ajoutée par rapport au groupe de travail, dont elle reprend les grandes orientations (paragraphe 1 des résolutions [75/240](#) et [77/37](#) de l'Assemblée générale). En outre, le mandat du programme d'action a été sensiblement restreint, puisqu'il consiste essentiellement à discuter des recommandations du groupe de travail et des groupes d'experts gouvernementaux, ainsi que des efforts de mise en œuvre déployés par les États.

Le renforcement des capacités, qui figure parmi les orientations mises en avant pour la promotion du programme d'action, fait également partie du mandat du groupe de travail. Celui-ci a dressé une liste de principes universels en la matière (rapport de 2021), tandis que, conformément à la résolution [77/36](#) de l'Assemblée générale, des échanges de vues sont déjà consacrés à la question des besoins des États et des moyens, y compris financiers, d'y répondre.

En outre, soucieux de donner un aspect pratique au programme d'action, ses auteurs s'approprient des propositions qui ont été soumises par des États et qui sont déjà en cours d'examen au groupe de travail. C'est notamment le cas de celle concernant la création d'un répertoire d'interlocuteurs et d'un portail numérique permanent de l'ONU consacré à la sécurité internationale de l'information. Ces propositions seront mises en œuvre (dès qu'elles feront l'objet d'un consensus de la part des États) indépendamment de l'exécution du programme.

Il importe de prendre en compte le fait que les pays occidentaux donnent un sens politique très précis au programme d'action et qu'ils en font publiquement un instrument contre la Russie. Ils justifient la nécessité de sa mise en place par des affirmations infondées concernant des activités prétendument malveillantes menées par notre pays dans le cyberspace, y compris dans le contexte de l'opération militaire spéciale en Ukraine (cet argument a notamment été avancé par la partie française à l'Organisation pour la sécurité et la coopération en Europe). Un discours antirusse de ce genre ne saurait servir de base à une coopération constructive entre États sur la question de la sécurité internationale de l'information. Il est contraire à l'esprit de la Charte des Nations Unies et en particulier à son article premier, où sont évoquées l'égalité et les relations amicales entre les nations. Dans ces conditions, on peut s'attendre à ce que les pays occidentaux utilisent le programme d'action pour imposer, à la place des normes du droit international, des règles qui les favorisent sans les obliger – dans le droit-fil de la conception d'un « ordre fondé sur les règles » promue par les États-Unis d'Amérique.

La Fédération de Russie considère qu'il faut commencer par codifier les règles volontaires existantes de comportement responsable dans un texte juridiquement contraignant à portée universelle, avant de discuter des moyens de demander aux pays de rendre compte de leur observation de ces règles. Un nombre croissant d'États sont favorables à la création d'un régime juridique international, à l'ONU, dans le domaine de la sécurité internationale de l'information. Quel que soit le format de négociation adopté à expiration du mandat du groupe de travail, il doit être consacré à l'élaboration de cet instrument.

C'est pourquoi, à la quatrième session du groupe de travail, la Russie a présenté sa conception d'une convention de l'ONU sur la sécurité internationale de l'information. Concrétisant de nombreuses années de discussions sur le sujet, cette conception est fondée sur les buts et principes énoncés dans la Charte des Nations Unies qui, reconnus par tous, unissent la communauté internationale en vue du

maintien de la paix et de la sécurité internationales. Elle approfondit les recommandations des résolutions annuelles de l'Assemblée générale sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale ainsi que celles figurant dans les rapports consensuels du Groupe de travail de 2021 et des groupes d'experts gouvernementaux de 2010, 2013, 2015 et 2021. Enfin, elle tient compte des initiatives des États incluses dans le document récapitulatif présenté par la présidence du premier Groupe de travail. Un texte de ce genre doit prévoir des mécanismes permettant de contrôler que les parties en respectent les termes, d'introduire des modifications et des ajouts, de favoriser l'échange de vues concernant la mise en œuvre du document et de régler pacifiquement les litiges.

Il va de soi que le groupe de travail est la plateforme la plus propice aux discussions concernant cette proposition et celle des autres pays en matière de sécurité numérique. Le groupe travaille dans l'intérêt de l'écrasante majorité des États Membres et ne doit donc pas être remplacé par le programme d'action. Les éléments du programme que les États jugeraient bénéfiques peuvent être intégrés dans le mécanisme actuel ou futur, à moins qu'ils ne le soient déjà.

Finlande

[Original : anglais]
[13 avril 2023]

I. Introduction : arguments généraux en faveur du programme d'action

La Finlande partage les préoccupations de nombreux États Membres concernant les cyberopérations malveillantes et nuisibles qui menacent la paix et la sécurité internationales.

La Finlande se félicite des progrès qu'ont accomplis les groupes de travail actuels, leurs prédécesseurs et les groupes d'experts gouvernementaux, notamment en formulant des constatations et des recommandations importantes, et, en particulier, en affirmant l'applicabilité du droit international au cyberspace et en élaborant un cadre de comportement responsable des États en matière d'utilisation du numérique qui a été approuvé par consensus par l'Assemblée générale dans ses résolutions [70/237](#) et [76/19](#).

Comme indiqué dans le rapport final du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, les États Membres 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 »²¹. Les États ont également souligné qu'il était « utile de réfléchir à des moyens de suivre [...] l'application [des règles et normes] qui ont déjà été convenues »²². Le programme d'action devrait donc mettre fortement l'accent sur l'appui apporté à la mise en œuvre du cadre normatif de comportement responsable des États en matière d'utilisation du numérique ainsi que sur son suivi.

Les États ont également fait observer que le cadre normatif était de nature cumulative et évolutive et que des normes supplémentaires pourraient être élaborées au fil du temps si des lacunes venaient à apparaître. La Finlande ne voit pas la nécessité de créer un nouvel instrument international juridiquement contraignant en

²¹ Voir [A/75/816](#), par. 74.

²² Ibid., par. 73.

la matière. Le programme d'action doit favoriser la mise en œuvre du cadre existant, mais il doit aussi faire en sorte qu'il puisse être amélioré, surtout lorsqu'on sait que de nouvelles menaces et de nouveaux problèmes pourraient apparaître.

Le programme d'action servirait dans ce contexte de mécanisme permanent et institutionnel de suivi de la mise en œuvre du cadre. Il permettrait en effet de formuler des séries de recommandations concrètes et de les mettre régulièrement à jour et d'appuyer ou de promouvoir des projets de renforcement des capacités menés dans ce domaine. Il resterait cependant flexible de façon à permettre les améliorations futures du cadre, selon qu'il convient.

II. Portée et objectifs

L'objectif principal du programme d'action serait de contribuer au maintien de la paix et de la sécurité internationales en assurant la préservation d'un environnement numérique ouvert, stable, sûr, accessible et pacifique.

À cette fin, les objectifs spécifiques du programme d'action devraient être les suivants :

- la coopération : réduire les tensions, prévenir les conflits et promouvoir l'utilisation du numérique à des fins pacifiques en adoptant une approche de coopération pour lutter contre les cybermenaces et en encourageant l'ouverture d'un dialogue inclusif entre les États ainsi qu'avec les parties prenantes concernées, notamment la société civile, le secteur privé, le monde universitaire et la communauté technique ;
- la stabilité : renforcer la stabilité dans le cyberspace en appuyant la mise en œuvre et l'amélioration, selon qu'il convient, d'un cadre de comportement responsable des États fondé sur le droit international, y compris le droit international humanitaire et les droits humains, ainsi que sur les normes de comportement responsable des États et les mesures de confiance et de renforcement des capacités ;
- la résilience : contribuer à la réduction des fractures numériques, en particulier celle qui existe entre les genres, ainsi qu'au renforcement de la résilience mondiale en ce qui concerne la mise en œuvre du cadre de comportement responsable des États.

III. Structure et teneur

Le programme d'action servirait de plateforme permanente pour l'instauration d'un dialogue institutionnel régulier auquel participeraient tous les États et toutes les parties prenantes concernées. Il fonctionnerait de manière transparente selon une approche axée sur les résultats et fondée sur le consensus.

La mise en place du programme d'action pourrait permettre de réaffirmer la volonté politique des États Membres à l'égard du cadre de comportement responsable des États et de favoriser la coopération entre les différentes parties prenantes. Le programme d'action offrirait par ailleurs la possibilité de promouvoir la mise en œuvre de ce cadre et d'y apporter des améliorations selon qu'il convient.

Pour ce qui touche à la structure du programme d'action, on pourrait s'inspirer d'autres exemples pertinents, comme le Traité sur le commerce des armes, et organiser des réunions annuelles pour examiner les travaux des groupes de travail techniques qui se réuniront entre les sessions.

Les décisions et les recommandations seraient adoptées par consensus lors des réunions annuelles sur la base des travaux intersessions réalisés par des groupes de

travail techniques chargés d'étudier des questions précises, comme les normes spécifiques et la mise en œuvre de ces normes ainsi que la manière dont le droit international s'applique à l'utilisation des technologies de l'information et des communications (TIC).

Le programme d'action et ses groupes de travail techniques seront inclusifs et permettront à tous les États qui le souhaitent de s'impliquer. La participation des experts gouvernementaux compétents sera encouragée, tout comme celle des parties prenantes concernées.

De nouveaux groupes de travail techniques pourraient être créés lors des réunions annuelles pour aborder les questions émergentes ou les nouvelles priorités.

Promouvoir la mise en œuvre du cadre

Le programme d'action encouragerait les États à signaler, à titre volontaire, les mesures qu'ils prennent pour mettre en œuvre le cadre en prévoyant la création de son propre système de communication de l'information ou la promotion des mécanismes existants, dont l'enquête de l'Institut des Nations Unies pour la recherche sur le désarmement sur l'application à l'échelle nationale des recommandations de l'ONU en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale. Ces rapports serviraient de base pour recenser les priorités dans le domaine de l'application des normes et permettraient de définir les besoins en matière de renforcement des capacités.

Le programme d'action pourrait prévoir l'adoption et la mise à jour régulière de recommandations concrètes concernant les efforts de mise en œuvre déployés au niveau national.

Le programme d'action permettrait d'appuyer les efforts de renforcement des capacités liés à la mise en œuvre du cadre et de renforcer la coopération multipartite dans ce domaine ainsi que la coordination avec d'autres initiatives pertinentes. Il servirait en outre de plateforme pour la mise en commun d'enseignements et d'expériences en ce qui concerne l'appui au renforcement des capacités et à la mobilisation de ressources et la mise en adéquation des ressources disponibles avec les demandes d'aide au renforcement des capacités.

Il devrait également offrir des possibilités de renforcer la complémentarité entre les acteurs, les processus et les mécanismes existants, notamment aux niveaux international et régional, et prévoir l'organisation de discussions ciblées avec les représentantes et représentants des organisations concernées.

Améliorer le cadre s'il y a lieu

De nouvelles normes pourraient être adoptées par consensus, selon qu'il convient, dans le cadre de réunions annuelles ou de conférences d'examen.

Faire participer de multiples parties prenantes

« Les États sont responsables au premier chef du maintien de la paix et de la sécurité internationales »²³ et ils ont donc un rôle central et un rôle décisionnel à jouer dans le programme d'action.

Par ailleurs, il est essentiel de resserrer encore la collaboration avec la société civile, le secteur privé, le monde universitaire et la communauté technique pour promouvoir le comportement responsable des États dans le cyberspace. Les groupes de travail précédents ont insisté à plusieurs reprises sur l'importance de resserrer la

²³ Ibid., par. 10.

collaboration entre les différentes parties prenantes²⁴, d'une part parce que l'exécution des engagements qu'ont pris les États au titre du cadre est tributaire de la coopération avec celles-ci, et d'autre part parce que les parties prenantes elles-mêmes « ont la responsabilité d'utiliser les TIC d'une manière qui ne mette pas en danger la paix et la sécurité »²⁵. La participation de multiples parties prenantes peut aussi contribuer aux efforts de renforcement des capacités.

Les modalités relatives au fonctionnement des groupes de travail et au déroulement des réunions du programme d'action devraient ainsi permettre aux parties prenantes d'assister aux sessions formelles, de faire des déclarations et d'apporter des contributions, comme c'est le cas dans d'autres processus de la Première Commission pour lesquels leur expertise s'est avérée utile, comme la réunion d'experts sur les systèmes d'armes létaux autonomes relevant de la Convention sur certaines armes classiques.

IV. Modalités et travaux préparatoires relatifs à la mise en place du programme d'action

Travaux préparatoires

Dans leurs rapports finaux, le Groupe de travail et les groupes d'experts gouvernementaux ont recommandé de poursuivre l'élaboration du programme d'action, notamment dans le cadre du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Le rapport annuel d'activité de l'actuel groupe de travail préconise également la tenue de débats ciblés sur le programme d'action.

En outre, il est prévu dans la résolution [77/37](#) que le rapport qui sera présenté à l'Assemblée générale par le Secrétaire général serve de base aux débats qui se poursuivront au sein du groupe de travail.

Des réunions intersessions et des sessions du groupe de travail devraient donc être organisées en 2024 et en 2025 pour poursuivre l'élaboration des différents aspects du programme d'action et rédiger le texte fondateur, entre autres.

Mise en place

Dans la résolution [77/37](#) de l'Assemblée générale, il est fait mention de la possibilité d'organiser une « conférence internationale » pour mettre en place le programme d'action, comme cela a été fait, par exemple, pour le Programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous tous ses aspects.

Une telle conférence internationale pourrait être organisée en 2025 ou en 2026 aux fins de l'adoption du texte fondateur du programme d'action sur la base des travaux préparatoires réalisés, notamment au sein du groupe de travail.

Cette conférence internationale devrait prévoir la participation des parties prenantes accréditées selon des modalités proches de celles adoptées dans la résolution [75/282](#) de l'Assemblée générale.

²⁴ Ibid., par. 22.

²⁵ Ibid., par. 10.

France

[Original : français]

[12 avril 2023]

I. Introduction

Les États reconnaissent depuis maintenant plus de 20 ans que le numérique est un catalyseur du progrès humain et du développement, mais qu'il peut également être utilisé à des fins incompatibles avec l'objectif de maintien de la stabilité et de la sécurité internationales.

Depuis 2003, la Première Commission de l'Assemblée générale a créé une série de groupes de travail qui ont œuvré au maintien de la paix, de la sécurité et de la stabilité internationales dans l'environnement numérique. À cette fin, ces groupes de travail ont consolidé un cadre relatif au comportement responsable des États dans l'utilisation du numérique, que l'Assemblée générale a approuvé par consensus dans plusieurs résolutions²⁶.

Ces groupes de travail ont également évoqué l'instauration d'un dialogue institutionnel régulier pour traiter les questions relatives à l'utilisation du numérique dans le contexte de la sécurité internationale.

Il a été souligné qu'un tel dialogue devrait s'attacher tout particulièrement à soutenir la mise en œuvre du cadre. En particulier, le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (2019-2021) a conclu que le futur dialogue institutionnel régulier « 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 »²⁷. Les États ont aussi souligné qu'il était « utile de réfléchir à des moyens de suivre [...] l'application [des règles et normes] qui ont déjà été convenues »²⁸.

Les États ont également fait observer que le cadre était de nature cumulative et évolutive et que des normes supplémentaires pourraient être élaborées au fil du temps. Ils ont par ailleurs pris note de la possibilité d'établir, à l'avenir, de nouvelles obligations contraignantes, le cas échéant²⁹. Le futur dialogue institutionnel régulier devra soutenir la mise en œuvre du cadre déjà convenu, mais également permettre une possible évolution de ce cadre à l'avenir, notamment dans un contexte d'émergence de nouveaux enjeux et menaces.

Dans ce contexte, la mise en place d'un programme d'action doterait la Première Commission d'un mécanisme institutionnel permanent qui assurerait le suivi de la mise en œuvre du cadre déjà convenu et qui rendrait possible, le cas échéant, son évolution.

II. Portée et objectifs

En tant que mécanisme de la Première Commission, le programme d'action porterait sur les questions relatives à l'utilisation du numérique dans le contexte de la sécurité internationale. Il aurait pour objectif principal de contribuer au maintien de la paix et de la sécurité internationales en préservant un environnement numérique ouvert, sûr, stable, accessible et pacifique.

²⁶ Voir les résolutions [70/237](#) et [76/19](#) de l'Assemblée générale.

²⁷ [A/75/816](#), annexe I, par. 74.

²⁸ [A/75/816](#), annexe I, par. 73.

²⁹ Résolution [76/19](#) de l'Assemblée générale, dixième alinéa.

À cette fin, les objectifs du programme d'action devraient être les suivants :

- la coopération : réduire les tensions, prévenir les conflits et favoriser l'utilisation du numérique à des fins pacifiques grâce à une approche coopérative pour faire face aux cybermenaces, ainsi qu'à un dialogue inclusif entre États et avec les parties concernées ;
- la stabilité : promouvoir la stabilité dans le cyberspace en soutenant la mise en œuvre et, le cas échéant, l'évolution du cadre de comportement responsable des États fondé sur le droit international, y compris le droit international humanitaire et les droits de l'homme, les normes relatives au comportement responsable des États, les mesures de confiance et le renforcement des capacités ;
- la résilience : contribuer à la réduction de la fracture numérique et au renforcement de la résilience au niveau mondial s'agissant de la mise en œuvre du cadre de comportement responsable des États.

III. Structure et contenu

Structure institutionnelle

Le programme d'action pourrait se fonder sur un document politique dont l'objectif serait, notamment, de :

a) réaffirmer l'engagement politique des États en faveur du cadre de comportement responsable des États, tel qu'affirmé dans les résolutions et les rapports pertinents³⁰. Cet engagement fondateur prendrait en compte les conclusions adoptées par consensus au sein du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), par exemple la création éventuelle d'un répertoire mondial et intergouvernemental des points de contact, la mise en place éventuelle d'un portail mondial de coopération ou encore la possibilité de créer un registre des menaces. Un futur programme d'action devra s'appuyer sur ces conclusions adoptées par consensus³¹ ;

b) établir un mécanisme institutionnel permanent visant à : i) favoriser la mise en œuvre de ce cadre, notamment en appuyant les capacités des États en la matière ; ii) continuer de faire évoluer le cadre, le cas échéant ; iii) encourager la coopération multipartite dans les domaines pertinents.

Le programme d'action, en tant que mécanisme permanent, pourrait adopter la structure institutionnelle suivante :

Organisation régulière de réunions, par exemple sur une base annuelle (la France est disposée à poursuivre les discussions sur la périodicité optimale des réunions du programme d'action, compte tenu des capacités des États et de la nécessité pour le programme d'action de suivre le rythme des évolutions dans le domaine du numérique). Ces réunions permettraient de : a) de discuter des menaces existantes et émergentes ; b) d'envisager la mise en œuvre des normes, règles et principes ; c) de poursuivre les discussions concernant la manière dont le droit international s'applique à l'utilisation du numérique et d'identifier les lacunes potentielles ; d) de discuter de la mise en œuvre de mesures de confiance ; e) d'identifier les priorités en matière de

³⁰ Notamment la résolution 76/19 de l'Assemblée générale, les rapports de consensus des groupes d'experts gouvernementaux de 2010, 2013, 2015 et 2021, le rapport de 2021 du Groupe de travail à composition non limitée (2019-2021) et le premier rapport d'activité du groupe de travail à composition non limitée (2021-2025), compte tenu du fait que les futures conclusions obtenues par consensus du groupe actuel enrichiront ce cadre cumulatif et évolutif.

³¹ Voir résolution 77/37 de l'Assemblée générale, deuxième alinéa.

renforcement des capacités, y compris sur la base d'informations fournies à titre volontaire ; f) d'identifier les futures mesures à prendre et de déterminer le programme de travail des réunions intersessions. Les réunions annuelles pourraient décider par consensus de créer des axes de travail techniques, ouverts à l'ensemble des États et des acteurs concernés, portant sur des points spécifiques (voir ci-dessous). La participation d'experts dans les domaines technique et juridique serait encouragée.

Organisation de réunions intersessions afin d'avancer dans le programme de travail convenu lors des réunions annuelles. Ces réunions pourraient être structurées autour d'axes de travail portant sur des points spécifiques, conformément aux priorités et aux domaines de travail identifiés lors des réunions annuelles.

Organisation de conférences d'examen, par exemple tous les quatre ans, permettant d'évaluer si le cadre doit être actualisé et, le cas échéant, de le faire évoluer (voir ci-dessous). Un axe de travail spécifique pourrait être créé pour approfondir les discussions sur la manière dont le droit international s'applique à l'utilisation du numérique et pour évaluer s'il existe des lacunes dans le cadre qui pourraient justifier de faire évoluer ce dernier.

Contenu

a) Promotion de la mise en œuvre du cadre

Le programme d'action encouragerait la communication volontaire d'informations sur les mesures prises au niveau national pour mettre en œuvre le cadre, soit par la création de son propre système de communication d'informations, soit par la promotion des mécanismes existants (tels que le modèle d'enquête nationale sur la mise en œuvre de l'Institut des Nations Unies pour la recherche sur le désarmement, ou encore les rapports nationaux présentés au Secrétaire général). Ces communications permettraient d'identifier les priorités en matière de mise en œuvre du cadre et d'évaluer les besoins en termes de renforcement des capacités.

Lors des réunions annuelles du programme d'action, il serait possible d'adopter et d'actualiser régulièrement des recommandations concrètes portant sur les efforts de mise en œuvre au niveau national. Conformément à la structure institutionnelle décrite ci-dessus, les réunions annuelles du programme d'action pourraient créer des axes de travail techniques ayant pour objectif de faire progresser les échanges sur certains aspects spécifiques liés à la mise en œuvre du cadre.

Par exemple, une priorité thématique pour la mise en œuvre du cadre pourrait être identifiée lors d'une réunion annuelle (mise en œuvre d'une norme ou d'une mesure de confiance particulière, sécurité des produits et des services numériques, protection des infrastructures essentielles, etc.). Pour procéder à de nouveaux échanges de vues sur cette question, la réunion annuelle pourrait alors décider de créer un axe de travail spécifique, dont les travaux auraient lieu lors des réunions intersessions du programme d'action et dont les conclusions seraient remises à la réunion annuelle suivante.

Le programme d'action soutiendrait les mesures de renforcement des capacités en ce qui concerne la mise en œuvre du cadre, et aurait pour objectif de renforcer la coopération multipartite en la matière ainsi que la coordination des efforts avec les autres initiatives pertinentes.

- Les États pourraient étudier la création, dans le cadre d'un futur programme d'action, d'un fonds de contributions volontaires pour financer certaines activités visant à promouvoir le cadre de comportement responsable des États. Un tel fonds pourrait s'inspirer de l'exemple du Mécanisme de financement des Nations Unies pour la coopération en matière de réglementation des

armements³². Les initiatives ou les projets financés par cet instrument devraient correspondre à un mandat, qui pourrait être défini lors de la première réunion du programme d'action (promotion de l'adhésion au cadre, respect des principes directeurs en matière de renforcement des capacités agréés dans le rapport final du Groupe de travail à composition non limitée (2019-2021), etc.) ;

- Le programme d'action aurait également pour objectif de valoriser les actions et les initiatives existantes. Les réunions du programme d'action et les réunions intersessions d'un groupe de travail technique sur le renforcement des capacités permettraient aux États d'échanger sur les priorités dans ce domaine (compte tenu des besoins identifiés grâce aux informations communiquées volontairement), et aux parties prenantes de présenter des initiatives pertinentes. Le programme d'action pourrait également élaborer un système de « certification » afin d'avaliser et de promouvoir les activités conformes à ses objectifs ;
- Les représentants d'autres organisations (Union internationale des télécommunications, fonds fiduciaire de la Banque mondiale pour la cybersécurité) pourraient présenter des exposés lors des réunions du programme d'action afin de garantir la coordination et la complémentarité entre les mesures de renforcement des capacités prises par les différentes structures (chacune agissant dans le cadre de son propre mandat et de son domaine de compétence).

b) Évolution du cadre

En tant que de besoin pour faire face aux nouveaux enjeux, les réunions régulières ou les conférences d'examen permettraient d'actualiser le cadre (en adoptant par exemple de nouvelles normes), sur la base du consensus.

c) Participation multipartite

Consciente du fait que « les États sont responsables au premier chef du maintien de la paix et de la sécurité internationales »³³ et qu'ils doivent conserver le rôle central qui est le leur (y compris l'exercice exclusif du pouvoir de décision) dans tout processus relevant de la Première Commission, la France appuie un dialogue et une coopération accrus avec les parties prenantes dans le cadre d'un futur programme d'action.

- La prise de décisions et la négociation des documents finaux demeureront une compétence exclusive des États ;
- Cependant, l'intérêt de renforcer encore la collaboration, le cas échéant, avec la société civile, le secteur privé, les universités et la communauté technique a été souligné à plusieurs reprises par les groupes de travail pertinents de la Première Commission³⁴. La coopération avec ces acteurs peut se révéler essentielle pour la mise en œuvre par les États de leurs engagements au titre du cadre de comportement responsable. En outre, ces parties prenantes ont elles-mêmes « la responsabilité d'utiliser les TIC [technologies de l'information et des communications] d'une manière qui ne mette pas en danger la paix et la sécurité »³⁵. Les acteurs privés peuvent également apporter un savoir-faire précieux aux échanges et contribuer aux efforts de renforcement des capacités ;

³² <https://www.un.org/disarmament/fr/unscar/>.

³³ A/75/816, annexe I, par. 10.

³⁴ A/75/816, annexe I, par. 22.

³⁵ A/75/816, annexe I, par. 10.

- Les modalités d'organisation des réunions du programme d'action doivent donc permettre aux parties prenantes de participer aux sessions officielles, de prononcer des déclarations et de présenter des contributions, comme c'est le cas dans d'autres processus relevant de la Première Commission où leur expertise est utile, notamment le Groupe d'experts gouvernementaux sur les systèmes d'armes létaux autonomes convoqué dans le cadre de la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination³⁶. Ces modalités, en permettant la tenue d'un dialogue multipartite dans un cadre officiel, favoriseraient une plus grande transparence du processus ;
- Pour garantir le caractère inclusif de ces réunions, la participation de parties prenantes de chaque groupe régional doit être encouragée et appuyée, notamment grâce à des programmes de parrainage spécifiques.

IV. Modalités et travaux préparatoires relatifs à la mise en place d'un programme d'action

Travaux préparatoires

La France est favorable à la poursuite de discussions ciblées et dédiées dans le cadre du groupe de travail à composition non limitée (2021-2025) pour continuer l'élaboration du programme d'action et rechercher un consensus en ce qui concerne sa mise en place.

Les rapports finaux du Groupe de travail à composition non limitée (2019-2021) et du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberspace dans le contexte de la sécurité internationale recommandent la poursuite de l'élaboration du programme d'action, notamment dans le cadre du groupe de travail à composition non limitée (2021-2025). Le rapport d'activité de 2022 de l'actuel groupe de travail à composition non limitée (2021-2025) appelle également à des discussions ciblées portant sur le programme d'action.

Dans sa résolution 77/37, l'Assemblée générale prévoit également que le rapport du Secrétaire général sur le programme d'action lui sera présenté et qu'il sera examiné par le groupe de travail à composition non limitée (2021-2025) en vue de la poursuite des discussions. De nombreux États ont insisté sur le fait que le groupe de travail à composition non limitée devrait constituer la principale enceinte pour l'élaboration du programme d'action dans la perspective de sa mise en place ultérieure.

Par conséquent, des réunions intersessions et des sessions spécifiques du groupe de travail à composition non limitée (2021-2025) devraient être organisées en 2024 et 2025 afin, notamment, de poursuivre l'élaboration des différents aspects du programme d'action et d'en rédiger le texte fondateur.

Mise en place

La France est favorable à la poursuite des discussions relatives à la façon précise dont le programme d'action sera éventuellement mis en place, en envisageant notamment l'option d'une conférence spécifique.

³⁶ Article 49 du Règlement intérieur de la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination (adopté dans le cadre de la cinquième Conférence des Hautes Parties contractantes chargée de l'examen de la Convention, en 2016).

La résolution 77/37 de l'Assemblée générale a évoqué une « conférence internationale » comme une option pour mettre en place le programme d'action (comme cela a notamment été le cas pour le programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous ses aspects). Si les États en décident ainsi, cette conférence internationale pourrait être organisée en 2025 afin d'adopter le texte fondateur du programme d'action, sur la base des travaux préparatoires accomplis dans le cadre du groupe de travail à composition non limitée (2021-2025).

Cette conférence internationale devra prendre ses décisions par consensus, à tout le moins en ce qui concerne les questions de fond. Elle devra permettre la participation des parties prenantes concernées (dont l'accréditation pourrait se faire selon des modalités proches de celles adoptées dans la résolution 75/282 pour le Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles).

L'Assemblée générale pourrait alors adopter une résolution saluant les résultats de la conférence et décider d'organiser la première réunion du programme d'action nouvellement créé.

Italie

[Original : anglais]
[14 avril 2023]

A. Introduction, motivations, portée et objectifs

L'Italie est résolument attachée au multilatéralisme et défend vigoureusement les travaux de l'Organisation des Nations Unies et l'instauration d'un dialogue institutionnel régulier sur la sécurité et l'utilisation des technologies numériques au sein de la Première Commission.

Le cadre international que l'Italie s'est engagée à respecter lorsqu'elle a adopté sa position sur le cyberspace se fonde sur les travaux des groupes d'experts gouvernementaux de 2010, 2013, 2015 et 2021 ainsi que sur ceux du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Ces travaux ont par ailleurs contribué à façonner la cyberarchitecture du pays. L'Italie s'engage à continuer d'en faire la promotion aux niveaux national et international.

Dans cette optique, l'Italie participe activement à l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), qui achèvera ses travaux en 2025, et considère la mise en place d'un programme d'action comme le meilleur moyen d'assurer un dialogue institutionnel régulier et efficace et d'ainsi contribuer à la poursuite de la mise en œuvre du cadre et des conclusions de l'actuel groupe de travail.

Le programme d'action devrait servir de structure/plateforme/mécanisme/forum unique et permanent permettant d'aborder les questions de cybersécurité au niveau mondial, en particulier dans le contexte de l'ONU. Le manque de capacités aux niveaux national, régional et mondial constitue un défi, et le programme d'action devrait appuyer les efforts qui sont faits à l'échelle nationale pour mettre en œuvre le cadre normatif et renforcer les capacités afin de contribuer à réduire la fracture numérique.

L'accélération de la transition numérique accroît les risques d'instabilité dans le cyberspace. À l'approche de la fin du mandat du groupe de travail, il est grand temps

d'entamer des discussions sur la mise en place du programme d'action, l'objectif étant de faire en sorte qu'elles puissent se poursuivre de manière plus structurée et plus prévisible après 2025.

B. Mécanisme

Puisqu'il convient d'éviter les doubles emplois, les discussions portant sur les buts, les objectifs, les principes, la structure, les fonctions, les modalités et la teneur du programme d'action devraient être menées dans le cadre du dialogue institutionnel régulier au sein de l'actuel groupe de travail. Des références au programme d'action devraient être insérées dans le prochain rapport annuel d'activité et les discussions sur un programme de travail pour 2024 et 2025 devraient commencer dès que possible.

Le rapport du Secrétaire général ayant un rôle crucial à jouer dans ce processus, il faudrait que les États aient plus de temps pour rédiger leurs contributions, selon que de besoin. On pourrait également envisager la possibilité d'adopter des résolutions techniques pour marquer les progrès réalisés chaque année jusqu'en 2025, date à laquelle une déclaration politique devrait également être soumise pour adoption à l'Assemblée générale. Une conférence spécifique pourrait être organisée après la fin du mandat de l'actuel groupe de travail, en 2025, pour faire avancer la mise en place du programme d'action et préparer le terrain pour la déclaration politique.

C. Principes, structure et teneur

Pour qu'une telle entreprise soit couronnée de succès, et compte tenu de la vitesse à laquelle les technologies numériques évoluent, le programme d'action doit être suffisamment flexible pour résister à l'épreuve du temps. Cela doit se refléter dans la fréquence à laquelle ses mécanismes sont réexaminés, ainsi que dans le nombre d'axes de travail techniques intersessions pouvant être créés ou supprimés.

Le groupe de travail a réussi à attirer l'attention de l'ensemble des États Membres de l'ONU sur l'utilisation des technologies de l'information et des communications. L'inclusivité devrait donc être la pierre angulaire des activités du programme d'action, tant en ce qui concerne la prise en compte des capacités de l'ensemble des États que la participation au débat des entités non gouvernementales. On devrait ainsi encourager les jumelages interrégionaux, les regroupements et la participation aux différents axes de travail et en faire des éléments essentiels du programme d'action. La nature intergouvernementale du processus décisionnel du programme d'action n'est pas remise en cause, mais la société civile et le secteur privé sont des acteurs essentiels du cyberspace et ils ont donc un rôle important à jouer dans tout dialogue institutionnel régulier réussi. Les modalités de fonctionnement actuelles des groupes de travail étant loin d'être satisfaisantes, il convient d'étudier de manière approfondie les moyens qui permettraient d'améliorer le niveau de détail et la fréquence des consultations multipartites en s'inspirant notamment des enseignements tirés d'autres processus.

Il faudra faire fond sur les succès des mécanismes et processus passés et présents pour adapter le programme d'action à la finalité qu'il poursuit. Le Bureau des affaires de désarmement devrait poursuivre l'excellent travail qu'il fait s'agissant d'assurer le secrétariat du programme d'action. On peut dire autant de bien du travail accompli par l'Institut des Nations Unies pour la recherche sur le désarmement, qui devrait continuer d'apporter sa contribution dans le cadre du programme d'action, non seulement en sa qualité d'institut de recherche, mais aussi lorsqu'il s'agit d'appliquer ses méthodes aux capacités d'analyse, de suivi et d'examen.

Le travail réalisé dans le domaine de la cybersécurité par les organisations régionales est fondamental. Cela devient de plus en plus évident lorsqu'on voit les efforts qui sont faits actuellement pour établir un répertoire mondial d'interlocuteurs, lequel constitue une première étape vers le renforcement de la coopération entre les États. Les possibilités de collaboration entre le programme d'action et les organisations régionales et sous-régionales devraient être examinées avec soin si l'on souhaite pouvoir accélérer les discussions sur certains sujets et disposer ainsi de plus de temps pour approfondir d'autres questions urgentes. Il faudrait par ailleurs étudier de manière approfondie les mécanismes permettant d'éviter qu'il y ait des redondances et que l'on prenne à nouveau des décisions ayant déjà été prises au niveau régional, l'idée étant de faire en sorte que le programme d'action soit aussi orienté vers l'action que possible.

Le succès du programme d'action dépend aussi de la régularité et de la prévisibilité des consultations organisées entre les États et les parties prenantes, dont on pourrait s'assurer par les moyens suivants : a) organisation à New York de conférences annuelles sur la mise en œuvre du cadre et les modifications qui pourraient y être apportées, ainsi que sur les travaux des axes de travail techniques ; b) organisation d'une conférence d'examen axée sur l'évaluation des résultats du programme d'action et sur son réexamen éventuel tous les quatre ans (Genève a été évoquée comme lieu possible pour l'accueil de la conférence) ; c) création d'axes de travail techniques ou thématiques qui se réuniraient de manière plus régulière ou plus fréquente, dont il sera décidé par consensus. Les discussions pourraient également se dérouler dans différents lieux géographiques ou dans un format hybride, à condition que les recommandations issues de ces activités soient validées au moins une fois par an lors de séances plénières. Les axes de travail techniques devraient se concentrer en priorité sur la mise en œuvre des acquis.

Un programme de travail biennal décrivant en détail les thèmes à aborder et les activités qu'il convient de mener devrait être présenté et approuvé à l'occasion de la conférence annuelle. Il devrait par ailleurs être accompagné d'un rapport établi par la présidence sur les activités menées au cours de l'année précédente. La personne qui assumera la présidence du programme d'action devrait être nommée pour un mandat de trois ans qui pourra être reconduit pour une durée d'un an. Un chevauchement de six mois avec le successeur ou la successeure serait souhaitable afin d'assurer la continuité du travail et de faciliter une transition en douceur.

Le groupe de travail devrait continuer de mener ses activités dans les domaines auxquels il s'intéresse actuellement (menaces existantes et potentielles, droit international, règles, normes et principes de comportement responsable des États, mesures de confiance et renforcement des capacités) dans le cadre du programme d'action. Celui-ci devrait, dans un premier temps, mettre l'accent sur la mise en œuvre de ce qui a été convenu par consensus dans le passé. Il faut par ailleurs accorder une attention particulière aux menaces vu le rythme soutenu des progrès techniques et les répercussions qu'ils ont. On pourrait envisager de créer un axe de travail supplémentaire consacré à un mécanisme volontaire d'examen par les pairs sur la mise en œuvre du cadre au niveau national. Les obligations ou les mécanismes actuels en matière de communication de l'information pourraient également être conservés afin de mettre sur pied des systèmes plus efficaces et moins chronophages à moyen et à long terme. Enfin, les débats sur la manière dont le droit international s'applique dans le cyberspace revêtent une importance cruciale, car ils permettent d'améliorer la compréhension des États, d'influencer leur comportement dans le cyberspace et de multiplier les possibilités de coopération mutuelle.

L'appui au renforcement des cybercapacités, qui devrait constituer l'un des éléments les plus importants du programme d'action, devrait être fourni sur demande

et sur la base des principes énoncés dans le document A/76/135. Le programme d'action pourrait absorber toute initiative en cours d'élaboration, à condition qu'elle contribue à faciliter l'analyse des possibilités de renforcement des cybercapacités, qu'elle ne duplique pas les initiatives en cours, qu'elle contribue à la désescalade des conflits et qu'elle prévienne la pratique qui consiste à rechercher la tribune la plus favorable. Il conviendrait d'étudier la possibilité de créer un mécanisme de financement spécifique en s'appuyant sur les expériences acquises dans le cadre des instruments existants fournis par des organisations régionales comme l'Union européenne ou des organismes spécialisés, dont le Fonds d'affectation spéciale multidonateur de la Banque mondiale pour la cybersécurité ou le Forum mondial sur la cyber expertise.

En ce qui concerne la participation aux différents axes de travail et aux différentes activités, il convient d'encourager les mécanismes visant à garantir l'équilibre géographique et la collaboration interrégionale. On pourrait par exemple exiger qu'un État Membre qui souhaite participer à un axe de travail soumette une demande conjointe avec un État Membre d'une autre zone géographique. On devrait par ailleurs envisager la création d'un mécanisme d'appui à la médiation pour aider les États Membres ayant des positions diamétralement opposées à s'entendre. Cet appui pourrait être fourni par l'ONU ou par les États Membres qui en ont le désir et la capacité et qui figurent sur une liste établie à cet effet. L'initiative pourrait s'inscrire dans le prolongement de l'axe de travail relatif aux mesures de confiance.

Japon

[Original : anglais]

[14 avril 2023]

1. Introduction

Le Japon est favorable à l'élaboration d'un programme d'action destiné à promouvoir le comportement responsable des États dans le cyberspace. Il estime qu'il s'agit là de l'occasion parfaite pour poursuivre les discussions à ce sujet. En tant que cadre orienté vers l'action, le programme d'action doit servir à appuyer les efforts que chaque pays déploie pour appliquer les normes et principes convenus en matière de comportement responsable, en favorisant le partage des meilleures pratiques et le recensement des difficultés propres à chaque pays.

Le programme d'action sera l'unique mécanisme de suivi de l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et sera mis en place pour appliquer les recommandations du groupe de travail à l'issue de son mandat. Il sera établi une fois le mandat de l'actuel groupe de travail terminé et ne visera pas à suivre une double approche.

Le Japon souhaite apporter la meilleure contribution possible aux discussions, en gardant à l'esprit que le programme d'action servira, comme il l'espère, à organiser la mise en œuvre effective des normes et principes convenus au niveau international.

2. Portée et objectifs

L'objectif du programme d'action est de contribuer 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 cette fin, le programme d'action doit viser en particulier à atteindre les objectifs suivants :

- a) Fournir des recommandations pour orienter les mesures prises au niveau national en vue d'appliquer les normes et principes de comportement responsable des États ;
- b) Encourager la communication, à titre volontaire, d'informations sur les pratiques nationales afin de recenser les besoins et les difficultés de chaque État Membre ;
- c) Appuyer, à la demande des pays bénéficiaires, les initiatives de renforcement des capacités, lesquelles sont adaptées aux besoins et aux difficultés des pays ;
- d) Être inclusif et assurer une large participation des États Membres et des parties prenantes.

En outre, le programme d'action constituera une plateforme permanente qui permettra d'avancer sur les questions récurrentes en facilitant les échanges sur les menaces existantes et émergentes, sur l'élaboration de mesures de confiance et sur la manière dont le droit international en vigueur s'applique au cyberespace.

3. Structure et teneur

a) Une structure visant à promouvoir la mise en œuvre du cadre

Les efforts déployés dans le cadre du Programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous tous ses aspects peuvent servir de référence pour préciser la portée, la structure et la teneur du programme d'action. Le Programme d'action relatif aux armes légères prévoit la prise de mesures spécifiques aux niveaux national, régional et international. Chaque pays présente ensuite, à titre volontaire, un rapport sur l'évolution de ses capacités juridiques et institutionnelles ainsi que sur d'autres pratiques, et organise une réunion d'examen annuelle.

S'agissant du programme d'action lié au cyberespace, le rapport volontaire devrait inclure une liste de contrôle destinée à suivre l'état de l'application des normes dans chaque pays, par exemple l'état d'avancement des mesures prises pour élaborer des politiques, des lois et des lignes directrices relatives à la protection des infrastructures critiques et la capacité d'intervention en cas d'incident dans chaque pays ou région. Il serait utile que chaque État Membre précise également ses besoins en termes de renforcement des capacités. Cet exercice devrait faciliter la mise en place d'un cadre destiné à appuyer les efforts déployés à l'échelle nationale pour mettre en œuvre les normes dans chaque pays.

La structure et les modalités du programme d'action devraient inclure l'organisation de conférences annuelles à l'ONU, au cours desquelles on serait en mesure d'adopter, et de mettre à jour régulièrement, des recommandations concrètes pour mettre en œuvre le cadre au niveau national. Par exemple, on pourrait, lors d'une conférence annuelle, définir une thématique prioritaire en vue de la mise en œuvre du cadre, telle que l'application d'une norme donnée, les menaces existantes et émergentes, la protection des infrastructures critiques, etc.

Pour favoriser les échanges à ce sujet, on pourra décider de créer un groupe de travail spécifique qui se réunirait lors des réunions intersessions des conférences annuelles du programme d'action et qui présenterait ses conclusions à la conférence annuelle suivante.

Le répertoire mondial d'interlocuteurs, qui doit être établi par l'actuel groupe de travail, ferait partie intégrante du programme d'action pour la mise en œuvre de mesures de confiance et l'élaboration de nouvelles mesures.

b) Renforcement des capacités

Le programme d'action permettrait d'appuyer les activités de renforcement des capacités menées pour mettre en œuvre le cadre, en garantissant la participation de toutes les parties prenantes.

Il serait utile, dans le cadre du programme d'action, que l'on recense les difficultés que les États Membres ont à mettre en œuvre le cadre et que l'on tire parti des initiatives existantes en matière de renforcement des capacités afin de résoudre ces difficultés.

Lors de réunions organisées dans le cadre du programme d'action, des représentantes et représentants d'autres organisations (par exemple, le Centre de renforcement des capacités en matière de cybersécurité de l'Association des nations de l'Asie du Sud-Est et du Japon, l'Union internationale des télécommunications et le Fonds d'affectation spéciale multidonateur de la Banque mondiale pour la cybersécurité) pourraient présenter des exposés afin de garantir la coordination et la complémentarité des activités de renforcement des capacités menées par chaque structure.

Le programme d'action devrait fonctionner comme une plateforme organisée sous les auspices de l'ONU afin de créer des synergies et de tirer parti des efforts déployés par d'autres organisations régionales, plutôt que de prévoir des programmes de renforcement des capacités qui lui seraient propres.

c) Droit international et normes internationales

En mai 2021, le Japon a présenté et publié la position fondamentale de son Gouvernement sur l'applicabilité du droit international aux activités menées dans le cyberspace, et le pays réaffirme que le droit international existant, y compris la Charte des Nations Unies dans son intégralité, est applicable aux cyberopérations. Il expose sa position actuelle sur la manière dont le droit international existant s'applique à ces activités, en se concentrant sur les questions les plus importantes et les plus fondamentales. Il continue d'espérer que l'annonce par les gouvernements de divers États de leur position de base sur l'applicabilité du droit international aux cyberopérations et l'application du droit international dans les cours et tribunaux nationaux et internationaux permettront d'approfondir la compréhension commune de la communauté internationale quant à la manière dont le droit international s'applique aux cyberopérations dans le cadre du programme d'action.

Le programme d'action encouragerait également les États à signaler, à titre volontaire, les mesures qu'ils prennent pour mettre en œuvre le cadre, soit grâce à la création d'un système de communication de l'information qui lui serait propre, soit grâce à la promotion des mécanismes existants (par exemple, l'enquête de l'Institut des Nations Unies pour la recherche sur le désarmement sur l'application à l'échelle nationale des recommandations de l'ONU en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale ou les rapports de pays présentés au Secrétaire général). L'établissement de rapports servira de base au recensement des priorités concernant la mise en œuvre du cadre et à la définition des besoins en termes de renforcement des capacités.

La conférence annuelle relative au programme d'action pourrait porter sur les moyens d'approfondir la question de l'application du droit international dans le cyberspace. Un axe de travail spécifique pourrait également être créé pour approfondir les échanges sur la manière dont le droit international existant s'applique aux activités menées dans le cyberspace.

4. Travaux préparatoires et modalités de mise en place du programme d'action

Le Japon est favorable à la tenue de nouvelles discussions ciblées au sein du groupe de travail afin de poursuivre l'élaboration du programme d'action.

Lettonie

[Original : anglais]
[14 avril 2023]

Le cadre de comportement responsable des États en matière d'utilisation du numérique est depuis longtemps – depuis 2003 – à l'ordre du jour de la Première Commission et fait l'objet de débats dans plusieurs groupes de travail, ce qui souligne l'importance croissante de l'utilisation responsable du numérique dans l'optique du maintien de la stabilité et de la sécurité internationales. La mise en place d'un programme d'action a été proposée comme moyen de promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le cadre d'une approche cohérente et à long terme. La résolution 77/37 de l'Assemblée générale sur le programme d'action – un mécanisme permanent, inclusif et orienté vers l'action – a reçu un large soutien parmi les États. Il faut donc poursuivre les discussions sur la portée, la structure, la teneur, les travaux préparatoires et les modalités de mise en place du programme d'action.

Avec la mise en place du programme d'action serait créé le premier mécanisme institutionnel permanent des Nations Unies axé sur l'utilisation responsable du numérique dans le contexte de la sécurité internationale. On garantirait ainsi la stabilité institutionnelle et des échanges réguliers sur les questions pertinentes, tout en évitant une éventuelle fragmentation du processus. Il convient de consacrer toute notre énergie et nos ressources au renforcement de la coopération et de la confiance entre les États, au lieu de discuter tous les deux ans des modalités d'un nouveau mécanisme.

L'idée d'établir un « dialogue institutionnel régulier » sous les auspices de l'ONU n'est pas nouvelle et a déjà fait l'objet de débats au sein de la Première Commission, comme indiqué, par exemple, dans le rapport final du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale³⁷. Le Groupe de travail a conclu que tout futur processus de dialogue institutionnel régulier mis en place 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 »³⁸. Comme indiqué dans la résolution 77/37 de l'Assemblée générale, le programme d'action « doit tenir compte des conclusions adoptées par consensus »³⁹ par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

Portée du programme d'action

Le programme d'action constituerait un mécanisme institutionnel permanent au sein de la Première Commission et une plateforme à laquelle tous les États pourraient participer. Il porterait sur les questions liées à l'utilisation du numérique dans le contexte de la sécurité internationale. Son objectif primordial serait de contribuer au renforcement de la paix et de la sécurité internationales et de promouvoir la prévention des conflits.

³⁷ Voir A/75/816.

³⁸ Ibid., par. 74.

³⁹ Résolution 77/37 de l'Assemblée générale, par. 2.

La coordination et les échanges entre les États et avec les parties prenantes concernées peuvent contribuer à prévenir les conflits, à dissiper les malentendus et à promouvoir un comportement responsable des États en matière d'utilisation du numérique. Le domaine de la cybernétique n'ayant pas de frontières et étant en constante évolution, il est essentiel de dialoguer pour faire face aux cybermenaces et aux difficultés existantes et potentielles.

Il est possible de renforcer la stabilité et la sécurité dans le cyberspace en appuyant la mise en œuvre et l'amélioration, selon qu'il convient⁴⁰, d'un cadre de comportement responsable des États fondé sur le droit international, y compris le droit international humanitaire et les droits humains, ainsi que sur les normes de comportement responsable des États et les mesures de confiance et de renforcement des capacités.

En vue de promouvoir la mise en œuvre du cadre de comportement responsable des États, on appuiera, dans le cadre du programme d'action, les activités de renforcement des capacités menées à cet égard. Il importe de collaborer davantage en matière de renforcement des capacités, en partageant notre expérience et nos meilleures pratiques avec les États qui ont besoin d'aide pour construire ou renforcer leurs cyberdéfenses, afin d'améliorer la résilience mondiale face aux cybermenaces.

Structure et teneur du programme d'action

Le programme d'action, en tant que mécanisme institutionnel permanent, favoriserait la mise en œuvre et l'amélioration, le cas échéant, du cadre de comportement responsable des États. Pour atteindre de tels objectifs, il doit soutenir les activités pertinentes de renforcement des capacités et favoriser le dialogue avec les parties prenantes.

On pourrait, dans le cadre du programme d'action, tenir des réunions chaque année et, entre ces réunions, organiser les travaux au sein de groupes de travail techniques consacrés à des questions spécifiques liées à la promotion d'un comportement responsable de l'État en matière d'utilisation du numérique. Par exemple, un groupe de travail technique pourrait s'efforcer de mieux comprendre comment le droit international s'applique à l'utilisation du numérique. Au cours des réunions annuelles, on adopterait les recommandations formulées par les groupes de travail techniques pendant l'intersession.

Ces groupes seraient créés et clôturés par une décision prise lors des réunions annuelles. Ils seraient inclusifs et ouverts à tous les États souhaitant y prendre part, et il faudrait s'assurer que les expertes et experts nationaux puissent participer en présentiel ou en ligne (format hybride). Les décisions relatives au nombre initial de groupes techniques, à la création de groupes techniques supplémentaires et à la fréquence de leurs réunions devraient être prises en tenant compte des capacités et des ressources de tous les États. Les recommandations préparées par ces groupes techniques devraient représenter les points de vue, les intérêts et les préoccupations du plus grand nombre possible d'États.

La coordination et les échanges avec les parties prenantes – la société civile, le secteur privé, les milieux universitaires et les milieux techniques – s'en retrouveraient favorisés, étant donné que leur expertise dans le domaine – en constante évolution – de la cybernétique est inestimable, que leurs activités contribuent à promouvoir le comportement responsable des États, et qu'elles ont elles-mêmes « la responsabilité

⁴⁰ Résolution 76/19 de l'Assemblée générale, dixième alinéa.

d'utiliser les technologies de l'information et des communications d'une manière qui ne mette pas en danger la paix et la sécurité »⁴¹.

Travaux préparatoires et modalités de mise en place du programme d'action

Nous pensons que l'Assemblée générale a accordé un mandat robuste pour procéder à la mise en place du programme d'action. Il faut poursuivre les discussions sur la portée, la structure, la teneur, les travaux préparatoires et les modalités de mise en place du programme d'action, et les organiser principalement au sein du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), comme le recommandent le Groupe de travail⁴² et le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberspace dans le contexte de la sécurité internationale⁴³ dans leurs rapports finaux. Par conséquent, il convient de consacrer suffisamment de temps aux discussions relatives au programme d'action au sein du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) lors des réunions intersessions et des sessions restantes. Les contributions nationales soumises conformément à la résolution 77/37 de l'Assemblée générale devraient servir de base à la poursuite des discussions sur l'élaboration du programme d'action.

Dans sa résolution 77/37, l'Assemblée générale a indiqué que l'organisation d'une conférence internationale⁴⁴ était une option qui permettrait aux États d'échanger leurs vues sur la mise en place du programme d'action. Une conférence internationale pourrait être convoquée en 2025 ou 2026 pour adopter le document fondateur du programme d'action, sur la base des travaux menés et des décisions prises par consensus au sein du groupe de travail.

Macédoine du Nord

[Original : anglais]
[14 avril 2023]

Communication du Gouvernement de la République de Macédoine du Nord faisant suite au rapport du Secrétaire général sur le programme d'action pour la mise en œuvre du cadre et le renforcement de la résilience conformément à la résolution 77/37 de l'Assemblée générale

Les échanges portant sur les principes liés au programme d'action sont essentiels pour renforcer notre capacité à relever les défis et à garantir un cyberspace sûr.

Nous pensons que la collaboration régionale et mondiale peut considérablement accélérer le rythme des efforts déployés par les acteurs étatiques pour améliorer leurs capacités de riposte et renforcer leur efficacité.

Dans les pays comparables à la Macédoine du Nord, où les normes et les ressources en matière de défense font défaut, les particuliers, les entreprises et les organisations sont très vulnérables aux cybermenaces. Par conséquent, le programme d'action devrait permettre d'établir une structure institutionnelle permanente et unifiée pour traiter les questions liées au cyberspace. Une telle structure devrait avoir

⁴¹ Voir A/75/816, par. 10.

⁴² Ibid., par. 77.

⁴³ Voir A/76/135, par. 97.

⁴⁴ Résolution 77/37 de l'Assemblée générale, par. 3.

un mandat clair et bien défini et être dotée de ressources suffisantes pour faire face à l'évolution constante des menaces.

Il faudrait également envisager d'améliorer la coopération interorganisations, y compris la collaboration interrégionale entre les institutions qui cherchent à renforcer leurs structures chargées des questions de cybersécurité, afin de renforcer la coordination, ce qui peut apporter une valeur ajoutée à l'échange d'expériences, le but étant de bâtir un front cohérent capable de régler tous les nouveaux problèmes.

Pour favoriser une large participation à cet égard, le programme d'action doit fournir un cadre souple et adaptable en fonction des besoins. À cet égard, le programme d'action pourrait prévoir l'organisation de séances plénières annuelles ou bisannuelles, ouvertes à tous les gouvernements, dont les décisions seraient fondées sur les travaux menés pendant l'intersession par les groupes de travail spécialisés.

Ces séances plénières pourraient également permettre de créer des groupes de travail se servant des connaissances des États et des parties prenantes concernées.

Si le cadre de comportement responsable des États établi doit servir de base aux travaux du programme d'action, il faut également prévoir la possibilité de l'actualiser si nécessaire. L'un des moyens d'y parvenir est de tenir des réunions plénières ou des conférences d'examen périodiques, au cours desquelles les États peuvent réévaluer le cadre et décider de l'améliorer, s'ils le jugent nécessaire. Pour garantir l'efficacité de ces examens, des groupes de travail spécialisés pourraient éclairer les travaux des réunions tenues en plénière pendant l'intersession.

Le programme d'action devrait viser en priorité, entre autres, à fournir un appui majeur aux activités menées, lequel pourrait prendre la forme de rapports volontaires sur les efforts de mise en œuvre déployés par les États participants, ce qui permettrait de recenser les besoins et les problèmes les plus urgents.

On devrait également, dans le cadre du programme d'action, fournir en permanence des recommandations pratiques actualisées pour aider les États à mettre en œuvre le cadre. En outre, on devrait offrir un appui aux activités de renforcement des capacités afin de permettre une mise en œuvre efficace.

Nous estimons que le programme d'action doit être complet et adapté à chaque pays. Toutefois, les besoins et les capacités des différents pays peuvent varier considérablement. Il importe donc que le programme d'action soit suffisamment souple pour tenir compte de ces différences et qu'il puisse être adapté aux besoins et aux contextes spécifiques de chaque pays. On garantirait ainsi la faisabilité et l'efficacité de sa mise en œuvre dans chaque contexte.

Le programme d'action doit donner la priorité à l'inclusivité, non seulement pour les États participants, mais aussi pour la communauté multipartite. En ce qui concerne les parties prenantes, le programme d'action devrait affirmer que les États sont les premiers responsables des questions liées à la sécurité internationale et qu'ils conservent donc le pouvoir de décision. Toutefois, il devrait également prévoir des modalités permettant à toutes les parties prenantes d'assister à des réunions, de faire des déclarations et de présenter des contributions écrites. On veillerait ainsi à la prise en compte des voix et des points de vue de toutes les parties concernées, tout en reconnaissant le rôle central des États en matière de sécurité internationale.

Monaco

[Original : français]

[14 avril 2023]

La Principauté de Monaco considère que le dialogue portant sur les moyens de réduire les risques d'instabilité, d'escalade et de dommages que fait peser l'utilisation malveillante des technologies de l'information et des communications sur la sécurité internationale doit se poursuivre au sein d'une structure institutionnelle permanente et unique. Cette structure institutionnelle ferait rapport à la Première Commission de l'Assemblée générale.

La recrudescence d'activités malveillantes dans le cyberspace, notamment les attaques contre les infrastructures critiques des États, nécessite un dialogue et une coopération à la fois réguliers et pérennes. L'établissement d'un programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale serait une plateforme appropriée. Il offrirait l'avantage de permettre une régularité des échanges à court, moyen et long terme et d'assurer une plus grande efficacité de ses actions en s'affranchissant de discussions liées au lancement de groupes de travail ainsi que de leurs mandats et produits livrables au sein de l'Assemblée générale.

Le programme d'action devra également offrir une certaine flexibilité afin de garantir la réactivité de ses membres à mesure de l'émergence de nouveaux défis dans une matière où les évolutions technologiques sont particulièrement rapides. Il devra ainsi permettre aux parties intéressées d'échanger sur les sujets qui les intéressent sur une base ad hoc avant d'en faire rapport à un organe plénier au sein dudit programme d'action.

En outre, afin de s'inscrire dans la continuité des travaux jusqu'alors réalisés et afin d'éviter toute duplication, il est essentiel que le programme d'action tienne compte des travaux menés sous les auspices des Nations Unies depuis une vingtaine d'années au sein des divers groupes d'experts gouvernementaux et groupes de travail. À cet égard, Monaco considère que le cadre du comportement responsable des États doit notamment en être le fondement. Le programme d'action devra également présenter un caractère dynamique permettant l'actualisation de ce cadre et de ses éventuelles évolutions, sur la base du consensus.

Par ailleurs, compte tenu de l'importance des activités du secteur privé, qui détient et exploite nombre de technologies de l'information et des communications à travers le monde, et de l'expertise et des capacités des organisations issues de la société civile sur ces sujets, le Gouvernement princier ne verrait que des avantages à permettre la participation de toutes les parties prenantes au programme d'action. Si le processus de décision doit demeurer une compétence exclusive des États, ceux-ci pourraient ainsi bénéficier des apports et expériences des diverses entités non étatiques. Ceci faciliterait la collaboration avec celles-ci, notamment afin de prévenir le développement d'outils malveillants et d'améliorer la sécurité du secteur, et contribuerait à la mise en œuvre du cadre de comportement responsable des États.

Il est en effet essentiel que le programme d'action soit orienté vers l'action, c'est-à-dire sur la mise en œuvre des normes de comportement responsable des États. À cet égard, la soumission de rapports de mise en œuvre, sur une base volontaire, serait particulièrement utile pour identifier les défis rencontrés et envisager les actions à entreprendre pour les relever. Par ailleurs, un échange de bonnes pratiques au niveau national, régional et international contribuerait à guider les États dans leurs actions.

Un programme d'action orienté vers l'action favorisera ainsi la coopération internationale et le renforcement des capacités des États, qui est primordial dans ce domaine : il conviendra de promouvoir les initiatives existantes et de renforcer leur coordination.

Enfin, le développement des mesures de confiance et le renforcement de la coopération internationale seront également essentiels à l'efficacité du programme d'action. Toutes les initiatives à cet égard, telles que le répertoire de points de contacts et diverses propositions permettant les échanges spécialisés dans ces domaines, devraient être encouragées.

Norvège

[Original : anglais]
[14 avril 2023]

La Norvège appuie la mise en place d'un programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. L'Assemblée générale s'est félicitée de la proposition de créer un tel programme d'action dans sa résolution 77/37, pour laquelle la Norvège s'était portée coauteur.

La Norvège estime que la mise en place d'un programme d'action est le meilleur moyen de faire avancer les débats et les activités de l'ONU en matière de cybersécurité et de comportement responsable des États dans le cyberspace. Elle est d'avis que le programme d'action devrait être une structure permanente permettant de traiter les questions de cybersécurité au sein de l'ONU. On pourrait ainsi mettre en place une structure stable permettant de se concentrer sur les activités orientées vers l'action et les progrès concrets, tout en poursuivant le débat normatif. Le programme d'action devrait réaffirmer l'importance du cadre consensuel de comportement responsable des États, établi après des années de discussions menées au sein des groupes d'experts gouvernementaux de 2010, de 2013, de 2015 et de 2021 et du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, et contribuer à le développer davantage. Il doit être inclusif, transparent, fondé sur le consensus, orienté vers l'action et axé sur les résultats.

Il nous faudrait disposer d'une structure unique au niveau de l'ONU, à la fois pour tenir un dialogue régulier et pour mettre en œuvre le cadre normatif de comportement responsable en matière d'utilisation du numérique. Le programme d'action devrait être établi d'ici à ce que le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) achève son mandat en 2025.

Le consensus obtenu sur le cadre normatif doit maintenant s'accompagner d'une mise en œuvre orientée vers l'action et d'un renforcement des capacités. Le programme d'action pourrait prévoir la promotion des activités de renforcement des capacités pour aider les États à mettre en œuvre le cadre normatif. Dans le cadre du programme d'action, les États Membres et les parties prenantes concernées pourraient organiser des discussions ciblées, des tables rondes et des réunions d'information sur leurs activités de mise en œuvre, le recensement des besoins et l'échange de connaissances, de bonnes pratiques et d'expertise, et les États pourraient établir des rapports à titre volontaire. Le programme d'action pourrait offrir une meilleure occasion d'apporter une assistance sur mesure aux États et ainsi de les aider à faire en sorte que le cyberspace demeure libre, ouvert et sûr. Il devrait tenir compte des initiatives qui sont actuellement menées et de la coopération existante en matière de

cybersécurité au sein des organisations concernées, telles que l'Organisation pour la sécurité et la coopération en Europe et d'autres organisations régionales.

Le programme d'action devrait être organisé de sorte à permettre une certaine flexibilité en termes de priorités et de mesures concrètes. Les États pourraient ainsi gérer l'apparition de nouvelles menaces et de technologies émergentes. Le programme d'action devrait être axé à la fois sur l'application des normes et sur la poursuite des échanges sur l'évolution du cadre normatif. La structure du programme d'action doit être réexaminée régulièrement, si nécessaire et approprié, dans le cadre de réunions régulières ou de conférences d'examen.

Le programme d'action doit être inclusif. Il importe que tous les États Membres puissent y prendre part. En outre, nous avons besoin d'une large participation des acteurs non gouvernementaux et des autres parties prenantes, car ils jouent un rôle important dans le maintien d'un cyberspace libre, ouvert et sûr. Des consultations régulières avec le secteur privé, les milieux universitaires et les organisations non gouvernementales permettraient d'obtenir l'expertise et les ressources nécessaires pour mener les débats voulus et prendre des mesures concrètes. L'inclusion de parties prenantes ne remet pas en cause le rôle que les États jouent dans la sécurité internationale.

La Norvège estime qu'il faudrait prévoir suffisamment de temps, dans le cadre du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), pour tenir des discussions approfondies sur les objectifs, les modalités et la mise en œuvre d'un futur programme d'action. Le groupe de travail devrait consacrer une session à l'examen du programme d'action.

Nouvelle-Zélande

[Original : anglais]
[12 avril 2023]

1. La cybersécurité fait l'objet de discussions entre les États, sous les auspices de l'ONU, depuis plus de 20 ans. Les groupes de travail successifs – groupes d'experts gouvernementaux et groupes de travail à composition non limitée – ont permis de tenir régulièrement des échanges sur les questions relatives à la cybersécurité dans le contexte de la sécurité internationale.
2. Les groupes de travail ont obtenu des résultats fondamentaux qui contribuent collectivement à la sécurité et à la stabilité internationales en établissant un cadre de comportement responsable des États dans le cyberspace, lequel a été approuvé par l'Assemblée générale et repose sur quatre piliers :
 - Droit international : tous les États Membres conviennent que le droit international s'applique au comportement des États dans le cyberspace.
 - Des normes de comportement responsable des États en ligne en temps de paix.
 - Des mesures de confiance destinées à promouvoir la transparence, la prévisibilité et la stabilité.
 - Des mesures de renforcement des capacités visant à garantir que tous les États peuvent limiter les risques associés au développement de la connectivité, sans rien perdre de ses avantages.
3. La Nouvelle-Zélande/Aotearoa estime qu'il est temps de s'appuyer sur cette base et de tenir un dialogue permanent, institutionnel et régulier sur la cybersécurité au niveau de l'ONU. En tant qu'auteur de la résolution [77/37](#) de l'Assemblée générale, elle appuie les discussions qui sont actuellement menées sur la mise en place

d'un programme d'action sur la cybersécurité et la poursuite de l'élaboration de sa portée, de sa structure, de sa teneur, de ses travaux préparatoires et de ses modalités, notamment dans le cadre du point de l'ordre du jour du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) consacré au dialogue institutionnel régulier.

4. La Nouvelle-Zélande/Aotearoa imagine un programme d'action qui soit le « foyer permanent » des discussions sur la cybersécurité à l'ONU à l'issue des travaux de l'actuel groupe de travail (2021-2025), en s'appuyant sur la proposition adoptée dans la résolution 77/37 de l'Assemblée générale. Conformément à cette proposition, elle soutient la mise en place d'un programme d'action :

a) Qui soit un mécanisme permanent d'organisation des discussions sur la cybersécurité au niveau de l'ONU après 2025, garantissant la prévisibilité et la stabilité institutionnelle. La négociation des modalités d'un mécanisme permanent permettrait également de réaliser des gains d'efficacité à long terme. Le réexamen et l'adoption des modalités pour les groupes de travail successifs ont nécessité des négociations longues et récurrentes, qui ont fait perdre du temps à d'importantes discussions de fond ;

b) Qui soit ancré dans le cadre concerté qui doit assurer un comportement responsable des États dans le cyberspace, y compris le droit international, et qui, ainsi, s'appuie sur les travaux fondamentaux des groupes d'experts gouvernementaux et des groupes de travail qui se sont succédé pour promouvoir le comportement responsable des États en ligne, et les renforce ;

c) Qui permette la participation des différentes parties prenantes, notamment les gouvernements (qui sont responsables de la paix et de la sécurité internationales dans le cyberspace), les entreprises, la société civile, les experts techniques, les universitaires et d'autres organisations qui contribuent à un Internet libre, ouvert, sécurisé et interopérable. La Nouvelle-Zélande/Aotearoa soutient les modalités qui prévoient la participation (y compris par des déclarations et la présentation de rapports écrits) des parties prenantes non gouvernementales aux discussions, et notamment aux réunions formelles et informelles et aux conférences d'examen ;

d) Qui soit orienté vers l'action, notamment en mettant l'accent sur la mise en œuvre du cadre de comportement responsable des États et en promouvant des mesures de renforcement des capacités qui aident les États à mettre en œuvre le cadre et les mécanismes de reddition des comptes et de contrôle ;

e) Qui soit flexible et adaptable, de sorte à gérer les technologies naissantes et à répondre aux menaces émergentes.

Pakistan

[Original : anglais]
[22 mars 2023]

Le Pakistan maintient une position cohérente et claire au sujet du dialogue institutionnel régulier, et notamment du programme d'action. Il propose que l'élaboration des futures plateformes de discussion sur le numérique repose, entre autres, sur les principes fondamentaux suivants : l'inclusivité, la transparence, la prise de décision par consensus, la participation de différentes parties prenantes, la collaboration à l'échelle mondiale et la durabilité. Il estime que le futur dialogue institutionnel doit également porter sur le renforcement des capacités, l'élaboration de normes et l'application du droit international dans le cyberspace, et inclure une discussion sur l'élaboration d'un instrument juridiquement contraignant visant à

réglementer le comportement des États dans le cyberspace. En outre, il est d'avis que ce dialogue devrait avoir lieu sous les auspices de l'ONU.

Il est essentiel de souligner qu'à ce stade, il n'est pas nécessaire de créer une structure parallèle au groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Le Pakistan est fermement convaincu que l'actuel groupe de travail est l'instance la plus appropriée pour toutes les discussions relatives au mandat et aux attributions de toute future plateforme, y compris le programme d'action.

La décision du Pakistan de s'abstenir de voter sur la résolution relative au programme d'action est motivée par sa conviction que tout mécanisme ou structure créé(e) après la conclusion, en 2025, des travaux de l'actuel groupe de travail doit reposer sur des bases durables et être élaboré(e) dans le cadre d'un processus consensuel. Le groupe de travail constitue donc une plateforme idéale pour ce type de discussion. Nous plaidons par conséquent en faveur d'une approche collaborative et globale du programme d'action, qui garantirait son efficacité et sa viabilité à long terme.

En outre, nous aimerions annoncer la présentation d'un document qui éclaire, en détail, la position du Pakistan sur l'application du droit international dans le cyberspace, y compris d'autres aspects de la cybersécurité à l'échelle mondiale. Le document peut être consulté à l'adresse suivante : https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/UNODA.pdf.

Pays-Bas (Royaume des)

[Original : anglais]
[14 avril 2023]

Introduction

Les Pays-Bas restent profondément préoccupés par le risque croissant que représente l'utilisation malveillante du numérique par des acteurs étatiques et non étatiques pour la sécurité et la stabilité internationales, le développement économique et social ainsi que la sécurité et le bien-être individuels. Ils notent également que le fait que les États ne disposent pas des mêmes capacités en matière de sécurité du numérique peut accroître la vulnérabilité dans un monde de plus en plus interconnecté.

Face à ces difficultés, les États ont élaboré, dans le cadre d'une série de processus intergouvernementaux, un cadre cumulatif et évolutif aux fins du comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. L'Assemblée générale a approuvé ce cadre à plusieurs reprises en adoptant des résolutions de consensus.

Pour faire fond sur ces réalisations, les Pays-Bas soulignent la nécessité d'établir un dialogue institutionnel régulier à l'issue des travaux de l'actuel 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. À cette fin, ils soutiennent l'initiative visant à établir un futur programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, initiative saluée par l'Assemblée générale dans sa résolution 77/37.

Conformément au paragraphe 3 de la résolution, la présente communication contient les vues des Pays-Bas sur la portée, la structure et la teneur du programme

d'action, ainsi que sur les travaux préparatoires et les modalités de sa mise en place. Le pays propose notamment de créer un mécanisme concret visant à faciliter le renforcement des capacités dans le cadre du programme d'action.

Portée et objectifs

Réaffirmant le paragraphe 1 de la résolution 77/37 de l'Assemblée générale, les Pays-Bas sont d'avis que le programme d'action devrait principalement viser : a) à renforcer les capacités des États et à appuyer les efforts qu'ils déploient pour mettre en œuvre et promouvoir les engagements pris au titre du cadre de comportement responsable ; b) à étudier ce cadre et à le développer, le cas échéant, sur la base d'un consensus. Tout en restant axé sur les questions liées à la paix et à la sécurité internationales, le programme d'action devrait également permettre de renforcer les synergies avec d'autres activités pertinentes, notamment celles liées à la cybercriminalité, à la connectivité, au renforcement des cybercapacités et au développement numérique.

Structure

Les Pays-Bas partagent l'idée selon laquelle le programme d'action devrait être un processus inclusif, transparent, fondé sur le consensus et axé sur les résultats. Son mandat pourrait découler d'un document fondateur, dans lequel les États affirmeraient leur engagement à respecter le cadre de comportement responsable dans le cyberspace, et par lequel serait établi un mécanisme permettant d'avancer dans la réalisation de ses objectifs.

Le programme d'action doit être inclusif et ouvert à la participation de tous les États Membres, des observatrices et observateurs permanents, des organisations intergouvernementales et autres, ainsi que des institutions spécialisées. En outre, si les États sont les premiers responsables du maintien de la paix et de la sécurité internationales, il devrait également permettre la participation significative, y compris dans des cadres formels, des parties prenantes non gouvernementales concernées, notamment le secteur privé, les milieux universitaires et la société civile.

Le programme d'action pourrait être structuré autour de réunions organisées régulièrement pour adopter des décisions et des recommandations par consensus, ainsi que de travaux entrepris au sein de groupes de travail techniques, ouverts à la participation des parties prenantes concernées et consacrés à des questions spécifiques, y compris une étude sur la manière dont les technologies nouvelles et émergentes affectent la paix et la sécurité internationales dans le cyberspace.

Teneur

Faciliter le renforcement des capacités dans le cadre du programme d'action permettra de promouvoir et de rationaliser la coopération internationale afin de faire progresser la mise en œuvre du cadre normatif à l'échelle mondiale. Le programme d'action pourrait également contribuer à créer des synergies avec les ressources existantes en matière de renforcement des capacités sur un ensemble plus large de questions liées à la cybernétique, telles que la connectivité, la lutte contre la cybercriminalité et les efforts plus généraux visant à réduire la fracture numérique.

Les Pays-Bas proposent notamment de mettre en place un mécanisme concret visant à faciliter le renforcement des capacités dans le cadre du programme d'action. Cette proposition repose sur un cycle de quatre étapes qui comprend : 1) la définition d'un ensemble de « domaines de renforcement des capacités » dans le cadre du programme d'action ; 2) une auto-évaluation et un recensement des besoins ; 3) la mise en adéquation des besoins et des ressources ; 4) un retour d'informations.

Étape 1 : définition d'un ensemble de « domaines de renforcement des capacités » dans le cadre du programme d'action

Dans le cadre du programme d'action, les États pourraient définir de concert un ensemble de « domaines de renforcement des capacités » approuvés qui sont essentiels à la mise en œuvre du cadre de comportement responsable des États. Une approche similaire a été adoptée pour définir des domaines d'assistance dans le cadre du Programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous tous ses aspects. Pour les domaines de renforcement des capacités, on s'appuierait sur les nombreuses orientations pratiques relatives à la mise en œuvre fournies dans les rapports de consensus du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberspace dans le contexte de la sécurité internationale, et on examinerait les domaines périodiquement de sorte à ce qu'ils restent à jour. Les domaines de renforcement des capacités fourniraient un cadre commun qui traduirait les résultats du consensus en mesures concrètes concernant, par exemple, la protection des infrastructures critiques, la réponse apportée en cas d'incident, les politiques et les stratégies, les équipes d'intervention informatique d'urgence, etc. Ils doivent également être flexibles de sorte à ce qu'on puisse les adapter aux différents contextes et priorités de chaque État. Pour déterminer les domaines de renforcement des capacités, les États pourraient s'inspirer des travaux entrepris par l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) sur l'adoption d'une approche fondée sur les menaces pour analyser les besoins en cybercapacités, de la liste récapitulative de normes à appliquer élaborée par Singapour et par le Bureau des affaires de désarmement, ainsi que des outils élaborés par d'autres parties prenantes, tels que le modèle de maturité des capacités en matière de cybersécurité pour les pays mis au point par l'Université d'Oxford.

Étape 2 : auto-évaluation et recensement des besoins

Sur la base des domaines de renforcement des capacités et de l'outil d'accompagnement, les États peuvent procéder, à titre volontaire, à une auto-évaluation afin de recenser leurs besoins et lacunes en matière de coopération et de renforcement des capacités. Cela garantirait la prise en main du cadre par les pays ainsi qu'une approche du renforcement des capacités fondée sur les besoins. L'enquête de l'UNIDIR sur l'application à l'échelle nationale des recommandations de l'ONU en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale est utile pour entreprendre une telle auto-évaluation. Les États peuvent ensuite choisir de partager les résultats de leur auto-évaluation dans le cadre du programme d'action, par exemple au sein d'un groupe de travail technique.

Étape 3 : mise en adéquation des besoins et des ressources

Ensuite, le programme d'action servirait de cadre de rencontre permettant de mettre en adéquation les besoins recensés en matière de renforcement des capacités et les ressources disponibles. Il permettrait aux fournisseurs d'aide au renforcement des capacités d'échanger avec les États à la recherche de ressources en la matière pour combler les lacunes recensées dans les domaines de renforcement des capacités. On encouragerait ainsi les fournisseurs à mettre à disposition des ressources consacrées aux domaines de renforcement des capacités, ce qui contribuerait à mobiliser davantage de ressources pour le renforcement des capacités dans un but commun. Le secrétariat pourrait aider les États en offrant en continu, en ligne, une vue d'ensemble des besoins en matière de renforcement des capacités et des ressources disponibles.

Cette vue d'ensemble intégrerait les outils existants, tels que le portail Cybil du Forum mondial sur la cyber expertise, ainsi que d'autres portails ou référentiels potentiels de l'ONU proposés par plusieurs États Membres au sein du groupe de travail. Une vue d'ensemble facilement accessible pourrait également aider les États à trouver les ressources disponibles pour renforcer leurs cybercapacités dans des domaines connexes de la sécurité internationale (par exemple, la cybercriminalité, le développement numérique, la connectivité, etc.). Il s'agit notamment des travaux de renforcement des capacités entrepris par des organisations régionales, l'Union internationale des télécommunications, INTERPOL, l'Office des Nations Unies contre la drogue et le crime et le Forum mondial sur la cyber expertise.

Les activités de renforcement des capacités menées dans le cadre du programme d'action devraient être entreprises conformément aux principes relatifs au renforcement des capacités adoptés par le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

Étape 4 : retour d'informations

Une fois que les besoins en matière de renforcement des capacités ont été recensés, qu'ils ont été mis en adéquation avec les ressources disponibles et que le renforcement des capacités est en cours, la plateforme du programme d'action faciliterait un retour d'informations pour rendre compte des progrès accomplis, partager les meilleures pratiques et déterminer dans quels domaines le cadre normatif pourrait être développé davantage.

Travaux préparatoires et modalités de mise en place du programme d'action

La résolution 77/37 de l'Assemblée générale fournit une première feuille de route pour la mise en place du programme d'action. Rappelant les recommandations figurant dans les rapports finaux du Groupe de travail et des groupe d'experts gouvernementaux selon lesquelles le programme d'action pourrait être élaboré plus avant dans le cadre du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), les Pays-Bas se félicitent de la poursuite des discussions sur la portée, la structure et la teneur du programme d'action au sein du groupe de travail et accueillent favorablement le paragraphe 2 de la résolution 77/37 de l'Assemblée générale, qui stipule que « le programme d'action doit tenir compte des conclusions adoptées par consensus par le groupe de travail à composition non limitée (2021-2025) ». À cet égard, ils encouragent le groupe de travail à tenir d'autres réunions intersessions et sessions consacrées à la poursuite de l'élaboration du programme d'action. Ils se félicitent également que l'Assemblée générale ait demandé au secrétariat du Bureau des affaires de désarmement, dans sa résolution 77/37, d'organiser une série de consultations régionales visant à échanger des vues sur le programme d'action.

En 2025, à l'issue des travaux du groupe de travail, les Pays-Bas envisagent d'organiser une conférence internationale, ouverte aux parties prenantes non gouvernementales, qui s'appuierait sur les travaux préparatoires réalisés, notamment au sein du groupe de travail, pour adopter le document fondateur.

Philippines

[Original : anglais]

[10 avril 2023]

Compte tenu de la nature évolutive des technologies de l'information et des communications dans le contexte de la paix et de la sécurité internationales, il est plus que jamais nécessaire de mettre en place un dialogue institutionnel régulier qui faciliterait la création d'une instance permanente pour tous les États Membres.

Les Philippines estiment que la mise en place d'un programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale est une bonne chose. Toutefois, elles sont d'avis que la mise en place d'un dialogue institutionnel régulier et permanent devrait être décidée par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Elles ont ainsi été contraintes de s'abstenir lors de l'adoption de la résolution 77/37 de l'Assemblée générale sur le programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale.

Les Philippines estiment que le groupe de travail est l'instance la plus appropriée pour discuter de la portée, de la structure et de la teneur du programme d'action, étant donné son mandat inclusif, transparent et consensuel. Selon le premier rapport annuel sur l'état d'avancement des travaux du groupe de travail, adopté par consensus, le groupe de travail a décidé de convoquer des réunions intersessions afin de faire avancer et d'approfondir les discussions portant sur des propositions spécifiques, y compris des propositions relatives à l'établissement d'un dialogue institutionnel régulier permanent sur la sécurité et l'utilisation du numérique. Ces réunions sont l'occasion pour les États Membres de mener un dialogue inclusif et de trouver des points de convergence sur l'avenir du dialogue institutionnel régulier.

Les Philippines réaffirment donc les principes énoncés au paragraphe 74 du document final adopté par consensus en 2021 par le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, selon lequel « 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, s'appuyer sur les réalisations précédentes et être inclusif, transparent, fondé sur le consensus et axé sur les résultats ».

Outre ces principes fondamentaux, les Philippines maintiennent que tout dialogue futur doit souligner qu'il importe de réduire la fracture numérique entre les genres, de promouvoir la participation véritable des femmes, notamment à des postes de responsabilité, aux processus décisionnels et de tenir compte des questions de genre.

Les Philippines réaffirment également la conclusion à laquelle est parvenu le groupe de travail au paragraphe 73 de son rapport de 2021, à savoir que le dialogue futur devrait, entre autres, sensibiliser l'opinion, instaurer la confiance et encourager des études et des discussions plus approfondies sur les domaines dans lesquels aucune communauté de vues ne s'est encore dégagée. Elles se joignent en outre aux États qui estiment qu'il est 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.

Par conséquent, les Philippines soutiennent l'idée d'un futur dialogue institutionnel régulier qui promouvoir un comportement responsable des États en

matière d'utilisation du numérique dans le contexte de la sécurité internationale, et dans le cadre duquel, entre autres :

- On mettrait en place des programmes de renforcement des capacités qui permettent aux États de mettre en valeur leurs compétences, leurs ressources humaines, leurs politiques et leurs institutions afin de faciliter leur participation véritable aux discussions sur les technologies de l'information et des communications dans le contexte de la sécurité internationale et de les aider à corriger les vulnérabilités de leurs infrastructures critiques. Les programmes de renforcement des capacités devraient se fonder sur les principes convenus par consensus par tous les États Membres dans le document final du groupe de travail (A/75/816), à savoir le processus, la finalité, les partenariats et les personnes, y compris l'intégration des activités de renforcement des capacités dans le Programme de développement durable à l'horizon 2030.
- On faciliterait la compréhension des menaces existantes et potentielles et de la manière d'y faire face.
- On fournirait des mesures concrètes sur la manière de mettre en œuvre les règles et normes existantes en matière de comportement responsable des États et on poursuivrait le débat sur d'autres normes possibles, compte tenu de l'évolution des menaces liées aux technologies de l'information et des communications, qui favoriseraient encore davantage la transparence et la prévisibilité du cyberspace et maintiendraient la paix dans ce domaine.
- On approfondirait la compréhension de l'applicabilité du droit international et, si des lacunes subsistent, on faciliterait une discussion au sein du groupe central sur la manière d'aborder cette question, par exemple en élaborant un document normatif ou un instrument juridiquement contraignant qui répondrait aux caractéristiques particulières de l'environnement numérique.
- On fournirait un guide pratique que les États pourraient utiliser pour faciliter le partage d'informations, les exercices de simulation et la coordination dans le domaine du numérique pour les questions liées à la paix et à la sécurité internationales.

Les Philippines estiment que le futur dialogue institutionnel sur le numérique dans le contexte de la sécurité internationale qui se tiendra régulièrement devrait être mis en place par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et qu'il ne devrait pas être lancé ni convoqué parallèlement aux travaux de l'actuel groupe de travail. Il convient d'éviter une multiplication des débats sur cette question importante, qui nuirait à la participation des petites délégations, à moins que le groupe de travail n'en décide autrement par consensus. Les discussions sur le futur dialogue devraient également prendre en compte les documents finaux des groupes de travail pour 2021 et 2025, les rapports d'activité annuels du groupe de travail et les rapports de 2010, de 2013, de 2015 et de 2021 du groupe d'experts gouvernementaux.

Roumanie

[Original : anglais]
[14 avril 2023]

Dans le droit fil des travaux menés sur la mise en place d'un « dialogue institutionnel régulier » pour traiter les questions liées à l'utilisation du numérique dans le contexte de la sécurité internationale, la mise en place d'un programme d'action permettrait à la Première Commission de se doter d'un mécanisme institutionnel permanent de suivi de l'application des normes convenues grâce à la

fourniture de séries de recommandations réalisables et à l'appui de projets pertinents de renforcement des capacités ou à leur promotion. La Roumanie estime qu'un tel mécanisme permanent, inclusif et orienté vers l'action est nécessaire de toute urgence.

La portée du programme d'action devrait être liée à l'utilisation du numérique dans le contexte de la sécurité internationale. Le programme d'action devrait viser à contribuer au maintien de la paix et de la sécurité internationales en préservant un environnement numérique ouvert, stable, sûr, accessible et pacifique, conformément au principe d'un comportement responsable des États dans le cyberspace.

Le programme d'action pourrait notamment viser à renforcer la coopération, à promouvoir la stabilité dans le cyberspace et à accroître la résilience. À cet égard, la réduction des tensions, la prévention des conflits, la promotion d'une démarche concertée au sujet des cybermenaces et l'appui à la mise en œuvre d'un cadre de comportement responsable des États fondé sur le droit international, y compris le droit international humanitaire et les droits humains, ainsi que sur les normes de comportement responsable des États et les mesures de confiance et de renforcement des capacités, ne sont que quelques-uns des objectifs à atteindre grâce à un dialogue inclusif entre les États et avec les parties prenantes concernées.

Le document politique du programme d'action devrait reposer sur la réaffirmation par les États de leur engagement en faveur du cadre de comportement responsable, sur la mise en place d'un mécanisme institutionnel permanent visant à promouvoir la mise en œuvre de ce cadre et sur la promotion de la participation des différentes parties prenantes, le cas échéant.

Conformément aux recommandations figurant dans les rapports du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et des groupes d'experts gouvernementaux sur l'élaboration du programme d'action, y compris dans le cadre du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), et conformément à la résolution 77/37 de l'Assemblée générale et aux dispositions relatives au rapport du Secrétaire général sur le programme d'action, des réunions intersessions et des sessions spéciales du groupe de travail devraient être organisées en 2024 et 2025 afin de poursuivre l'élaboration des différents aspects du programme d'action.

La Roumanie est d'avis que, conformément à l'option mentionnée dans la résolution 77/37, une conférence pour la mise en place du programme d'action devrait être convoquée dans les plus brefs délais.

Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

[Original : anglais]
[14 avril 2023]

Introduction

1. Au cours des 30 dernières années, les États Membres ont constitué un cadre de comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, qui a été approuvé par l'Assemblée générale dans diverses résolutions (entre autres les résolutions 70/237 et 76/19).
2. Le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale a conclu que tout futur processus de dialogue institutionnel régulier « 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 »⁴⁵.

3. En 2022, l'Assemblée générale, dans sa résolution 77/37, a voté en faveur de la création d'un programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. Le Royaume-Uni soutient fermement cette décision, qui vise à instaurer un mécanisme permanent, inclusif et orienté vers l'action, favorisant les discussions sur la paix et la sécurité internationales dans le cyberspace.

4. Au cours de l'élaboration du programme d'action, il convient de mettre l'accent sur :

a) **L'inclusivité.** Le programme d'action devrait être le fruit du travail et de la contribution de tous les États Membres. Il devrait permettre la participation active d'acteurs non gouvernementaux, selon des modalités définies. Le fait que le programme d'action devienne l'unique mécanisme à prendre la suite de l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) aidera les États à allouer efficacement des ressources à leurs activités connexes.

b) **La légitimité.** Les États Membres sont convenus d'un cadre destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. Il faut le prendre comme point de départ. Il est clair que le programme d'action doit aider les États à appliquer ce cadre consensuel et à mettre en évidence les moyens par lesquels le droit international en vigueur s'applique au cyberspace.

c) **La flexibilité.** L'attention portée à la mise en œuvre du cadre convenu devrait permettre de repérer les lacunes avant un prochain remodelage. Le programme d'action doit donc avoir une structure suffisamment flexible pour intégrer des correctifs au cours du temps et pour étoffer le cadre évolutif, notamment face aux nouvelles menaces.

Portée et objectifs

5. De manière générale, le programme d'action devrait avoir pour but de contribuer à la paix et à la sécurité internationales en défendant un cyberspace libre, ouvert, pacifique et sûr. Cela implique de faciliter le dialogue et la coopération entre États Membres sur les questions de sécurité et d'utilisation du numérique et d'appuyer la mise en œuvre et l'enrichissement du cadre.

6. Le programme d'action devrait être le seul mécanisme à prendre la suite de l'actuel groupe de travail en ce qui concerne les discussions relatives à la sécurité et à l'utilisation du numérique. Ainsi conçu, il offrirait :

- Des occasions de discuter des cybermenaces et de partager les informations sur le sujet (par exemple, aux réunions annuelles et dans les séances de travail spécialisées, où peuvent être examinés les nouveaux mécanismes de riposte tels que le portail proposé par l'Inde) ;
- Un moyen d'aider les États à recenser les domaines dans lesquels améliorer les capacités et la mise en œuvre du cadre (par le biais de rapports soumis volontairement ; en évaluant les activités de renforcement des capacités déjà menées par les organismes des Nations Unies ; en impliquant activement les acteurs non gouvernementaux tels que les organisations régionales, la société

⁴⁵ Voir A/75/816, par. 74.

civile et le secteur privé ; en collaborant avec le Fonds d'affectation spéciale multidonateur de la Banque mondiale pour la cybersécurité, etc.) ;

- Un processus inclusif permettant d'étoffer le cadre (notamment en axant le travail sur l'application du droit international au cyberspace) ;
- Une base en vue d'élaborer de nouvelles mesures de confiance (par exemple, en s'appuyant sur les répertoires d'interlocuteurs, un mécanisme permanent déjà en cours d'élaboration au groupe de travail actuel, et sur des discussions concernant les mesures à prendre en lien avec le forum permanent de l'ONU sur la paix et la sécurité internationales dans le cyberspace).

Structure et teneur

Déclaration politique

7. Le lancement du programme d'action devrait s'accompagner d'une déclaration politique convenue politiquement lors d'une réunion de haut niveau ou une conférence internationale. Le cadre devrait former la base de cette déclaration qui inclurait un accord sur les mesures visant à promouvoir le respect des engagements en matière de comportement responsable des États dans le cyberspace, expliciterait les moyens d'appliquer le droit international dans le cyberspace et définirait la portée et les modalités du programme d'action.

8. L'accord politique donnerait aux États l'occasion de réaffirmer leurs engagements de manière publique et explicite, à cette étape de l'élaboration du cadre, et de renforcer l'adhésion sur la scène intérieure.

9. La déclaration politique devrait accorder une large part au renforcement des capacités, qui est un élément important du cadre. En la matière, elle devrait tenir compte des principes du groupe de travail ainsi que du résultat des travaux effectués par d'autres organes des Nations Unies et par des acteurs extérieurs à l'Organisation, tels que les principes énoncés dans le communiqué de Delhi du Forum mondial sur la cyber expertise.

Réunion annuelle

10. Le programme d'action devrait prévoir la tenue d'une réunion officielle annuelle, qui serait l'occasion :

- De discuter des menaces nouvelles et émergentes et de partager les informations sur le sujet ;
- D'examiner la mise en œuvre du cadre, y compris sur la base des rapports soumis volontairement ;
- De partager des idées concernant le renforcement des capacités et d'assister à des présentations faites par des parties prenantes ;
- D'approfondir la compréhension du cadre, notamment concernant l'application du droit international ;
- D'examiner les recommandations formulées dans le cadre des différents axes de travail (qui pourraient être fixés lors des réunions annuelles).

Conférences d'examen

11. Les conférences d'examen devraient avoir lieu tous les quatre ans. Ce serait l'occasion de dresser un bilan du programme d'action et d'adapter ce dernier en fonction de la nature mouvante et évolutive des menaces contre la paix et la sécurité internationales dans le cyberspace.

Rapports volontaires

12. La mise en œuvre du cadre et le renforcement des capacités ont été placés en tête des priorités du programme d'action. La soumission de rapports volontaires viendra les appuyer. Les enquêtes existantes (comme l'enquête sur l'application à l'échelle nationale des recommandations de l'Organisation des Nations Unies en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale, de l'Institut des Nations Unies pour la recherche sur le désarmement) et les mécanismes évolutifs (telle la liste récapitulative des normes à appliquer, proposée par Singapour) posent les bases possibles d'une approche cohérente à l'échelle du programme d'action.

Participation multipartite

13. Seuls les États Membres devraient avoir le droit de négocier des textes et de prendre des décisions dans le cadre du programme d'action. Cependant, le point de vue des parties prenantes non étatiques demeure précieux. Celles-ci sont souvent les premières touchées par les cyberincidents, et elles jouent un rôle de premier plan dans la riposte ainsi que dans le renforcement des capacités. Elles devraient donc avoir la possibilité de participer activement à toutes les réunions prévues par le programme d'action, y compris par le biais de déclarations orales ou écrites. Cette participation devrait être ouverte à toutes les parties dans leur diversité, et il convient d'encourager l'expression des points de vue régionaux. Les modalités d'accréditation des parties devraient être transparentes, l'ensemble des États se prononçant sur les décisions finales – y compris à l'occasion d'un vote lorsqu'aucun consensus ne serait trouvé.

Travaux préparatoires et modalités

14. Le groupe de travail devrait se voir accorder un rôle important dans l'enrichissement du programme d'action. Eu égard au manque de ressources que connaissent les délégations, il devrait consacrer une partie de ses réunions formelles et informelles à examiner et à étoffer le programme d'action. L'importance de la tâche implique probablement la tenue de réunions entre les sessions.

15. En outre, les États Membres doivent conserver la possibilité de formuler des propositions lors de conférences supplémentaires et de les soumettre à l'examen du groupe de travail et de l'Assemblée générale.

Singapour

[Original : anglais]

[14 avril 2023]

Singapour attache une grande importance aux formulations consensuelles qui figurent jusqu'à présent dans le projet de programme d'action. Elles constituent une bonne base pour la poursuite de l'examen du texte. À cet égard, les éléments suivants, issus des précédents rapports de consensus des groupes de travail, demeurent importants :

- Comme mentionné dans 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, les États prennent note d'une série de propositions visant à promouvoir le comportement responsable des États en matière de technologies de l'information et des communications et qui renforceraient notamment la capacité des États à honorer les engagements qu'ils ont pris en matière d'utilisation du numérique, 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'égalité de 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 sur la sécurité du numérique et de son utilisation (2021-2025) créé en application de la résolution 75/240 de l'Assemblée générale⁴⁶.

- Dans son premier rapport d'activité annuel, le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) fait valoir qu'il est recommandé aux États de continuer de mener des discussions ciblées, aux quatrième et cinquième sessions du groupe de travail, afin d'étoffer le programme d'action en vue de sa mise en place en tant que mécanisme visant à promouvoir un comportement responsable des États en matière d'utilisation du numérique, ce qui permettrait notamment de les aider à honorer les engagements pris dans ce domaine. Lors de ces sessions, les États participeront également à des discussions ciblées sur la relation entre le programme d'action et le groupe de travail, ainsi que sur la portée, le contenu et la structure du programme d'action⁴⁷.

Tandis que les États Membres mènent des discussions ciblées dans le cadre du groupe de travail afin d'étoffer le programme d'action, et dans le contexte des échanges portant sur le futur processus de dialogue institutionnel régulier, Singapour estime que ce processus devra par nature être universel, inclusif, transparent, basé sur le consensus, orienté vers l'action et à voie unique. Concernant sa portée, son contenu et sa structure, il devrait respecter les principes de base suivants :

- Reposer exclusivement sur le consensus afin que soient préservés les accords fragiles obtenus de haute lutte par la communauté internationale dans le cadre des groupes d'experts gouvernementaux et groupes de travail successifs.
- Être mû par la volonté de bâtir sur les fondations posées par les travaux des groupes d'experts gouvernementaux et groupes de travail successifs.
- Tendre à renforcer le cadre cumulatif et évolutif de comportement responsable des États en matière d'utilisation du numérique et à réaffirmer l'esprit de consensus qui le sous-tend.

Slovénie

[Original : anglais]
[13 avril 2023]

La Slovénie considère le programme d'action relatif à la sécurité du numérique comme un instrument important qui devrait garantir la paix et la stabilité dans le cyberspace. En outre, il pourrait servir de vecteur efficace permettant au cyberspace de se développer, à l'avenir, de manière stable et ouverte.

Le programme d'action pourrait également offrir une structure permanente favorisant le traitement des problèmes liés au cyberspace à la Première Commission, et soumettre à l'Assemblée générale des mesures à prendre après adoption et approbation. La structure permanente serait un gage de stabilité institutionnelle et pourrait épargner à l'Assemblée générale les discussions sur la création des groupes de travail à composition non limitée, dont le mandat est, par définition, limité dans le temps. En tout état de cause, elle agirait en complément d'autres mécanismes de

⁴⁶ Voir A/75/816.

⁴⁷ Voir A/77/275.

l'ONU et en coordination avec ceux-ci, tel le 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](#).

La Slovénie est résolument favorable au principe d'une approche multipartite transparente et inclusive et à la participation d'acteurs étatiques et non étatiques aux diverses activités du programme d'action.

La Slovénie soutient que les États devraient réaliser des auto-évaluations à titre volontaire et être prêts à mettre en commun leurs pratiques exemplaires. Le programme d'action devrait favoriser le renforcement des capacités et le partage des informations de sorte que tous les États promeuvent et appliquent le cadre de comportement responsable dans le cyberspace. Le renforcement des capacités concernerait la réaction rapide, l'élaboration des politiques et des stratégies, la formation d'équipes d'intervention informatique d'urgence, la création des infrastructures numériques nécessaires, la législation et d'autres domaines majeurs. Le programme d'action devrait aussi être assez flexible pour permettre aux États de faire face aux nouvelles menaces et d'étoffer leur législation en cas de besoin.

Suède

[Original : anglais]

[14 avril 2023]

Introduction

La Première Commission a consolidé un cadre de comportement responsable des États en matière d'utilisation du numérique que l'Assemblée générale a approuvé par consensus dans plusieurs résolutions⁴⁸. À cet égard, des discussions ont porté sur la mise en place d'un dialogue institutionnel régulier destiné à résoudre les problèmes relatifs à l'utilisation du numérique dans le contexte de la sécurité internationale. Il a été souligné qu'un tel dialogue devrait s'attacher tout particulièrement à soutenir la mise en œuvre du cadre. En particulier, le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale a conclu que tout futur processus de dialogue institutionnel régulier « 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 »⁴⁹. Dans ce contexte, la mise en place d'un programme d'action fournirait un mécanisme institutionnel permanent permettant de suivre la mise en œuvre du cadre déjà convenu tout en autorisant sa possible modification, en fonction des besoins.

Teneur

Le programme d'action pourrait être basé sur un document politique dont les principales orientations seraient : a) réaffirmer l'engagement politique des États envers le cadre de comportement responsable, tel qu'affirmé dans les rapports et résolutions correspondants⁵⁰, ce qui prendrait en compte les décisions adoptées par

⁴⁸ Voir les résolutions [70/237](#) et [76/19](#) de l'Assemblée générale.

⁴⁹ Voir [A/75/816](#), par. 74.

⁵⁰ Cela comprend la résolution [76/19](#) de l'Assemblée générale, les rapports de consensus de 2010, 2013, 2015 et 2021 des groupes d'experts gouvernementaux, le rapport de 2021 du Groupe de travail à composition non limitée ([A/75/816](#)) et le premier rapport d'activité annuel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) ([A/77/275](#)). Les futures conclusions adoptées par consensus par le groupe de travail actuel enrichiront ce cadre, qui est cumulatif et évolutif.

consensus au Groupe de travail ; b) établir un mécanisme institutionnel permanent visant à : i) favoriser la mise en œuvre du cadre, notamment en appuyant les capacités des États en la matière ; ii) continuer de faire évoluer ce cadre, en fonction des besoins ; iii) encourager la coopération multipartite dans les domaines correspondants.

La Suède constate qu'il existe de nombreuses manières de favoriser la mise en œuvre du cadre. Elle rejoint la position de l'Union européenne et s'associe à la proposition française présentée au Groupe de travail en mars 2023. Elle contribue à la discussion en mettant l'accent sur l'importance d'adopter une stratégie multipartite, sur le rôle du secteur numérique privé et sur la nécessité de promouvoir les partenariats public-privé.

Participation multipartite

Étant donné que les États sont responsables au premier chef du maintien de la paix et de la sécurité internationales⁵¹, le programme d'action devrait favoriser la concertation et la coopération multipartites pour un cyberspace mondial ouvert, libre, stable et sûr.

À l'heure actuelle, les autorités nationales peinent parfois à trouver les moyens et les capacités d'analyser et de traiter le nombre croissant de menaces liées au cyberspace auxquelles leur pays doit faire face. Elles s'appuient de plus en plus sur la coopération et la collaboration avec le secteur privé et les autres acteurs non gouvernementaux afin d'apporter des réponses aux menaces et aux défis ainsi qu'aux besoins et aux préoccupations qui en découlent pour les politiques publiques. Dans le même temps, les groupes de travail de la Première Commission ont souligné l'intérêt de renforcer encore la collaboration, le cas échéant, avec la société civile, le secteur privé, les universités et la communauté technique⁵², à la fois parce que cela peut être décisif pour la mise en œuvre des engagements des États et parce que ces parties prenantes ont elles-mêmes « la responsabilité d'utiliser les technologies de l'information et des communications d'une manière qui ne mette pas en danger la paix et la sécurité »⁵³. En outre, du fait de leurs compétences, les acteurs privés peuvent apporter un éclairage précieux aux échanges et contribuer au renforcement des capacités. Les États ne peuvent garantir seuls la sécurité à l'ère du numérique, et l'approche multipartite doit demeurer un élément fondamental de la coopération.

Le rôle du secteur numérique privé dans la défense et la promotion des droits humains

Le secteur numérique a souvent été perçu comme un allié dans la défense de la liberté d'expression et des droits humains. Les téléphones et la technologie mobile relient les personnes et les entreprises. Internet offre une ouverture vers un nouveau monde d'informations, de formations et de divertissements, et facilite les échanges, les débats, les discussions, les négociations et la recherche de solutions. Les entreprises privées fournissent les technologies qui forment la colonne vertébrale d'Internet.

Le secteur numérique privé se caractérise par sa diversité. Il comprend les fournisseurs de matériel (pylônes, instruments et équipements, serveurs, câbles et autres éléments d'infrastructure), de logiciels et de services, ce qui inclut les nombreuses technologies et normes qui font l'architecture d'Internet. Cette diversité rend difficile toute approche globale du secteur et empêche également d'isoler un

⁵¹ Voir [A/75/816](#), par. 10.

⁵² *Ibid.*, par. 22.

⁵³ *Ibid.*, par. 10.

ensemble spécifique de problèmes. Comme dans d'autres domaines, le secteur numérique repose sur des entreprises du monde entier ; les stratégies concentrées sur des zones géographiques précises sont donc peu efficaces, au contraire des approches multilatérales, qui sont nécessaires.

L'obligation faite aux États de respecter les droits humains implique celle de protéger les personnes et les groupes contre les atteintes aux droits humains commises par des tiers, y compris des entreprises commerciales. Cela signifie que les États doivent introduire des mesures d'action positive qui facilitent l'exercice des droits humains fondamentaux (Principes directeurs relatifs aux entreprises et aux droits de l'homme, principe 1). Il est possible qu'un écart entre les attentes des utilisateurs et utilisatrices et de la société civile et la compréhension que les entreprises ont de leurs responsabilités subsiste toujours. Mais il faut parvenir à un consensus élargi, tant au niveau politique que sectoriel, afin de travailler sur ce sujet.

Des initiatives multipartites pour avancer

Pour relever les défis qui se présentent, les autorités nationales et les entreprises numériques ont besoin d'orientations solides basées sur des standards, des normes et des principes internationalement acceptés. La Suède continuera de promouvoir un cyberspace mondial libre, ouvert, stable et sûr dans lequel les droits humains, les libertés fondamentales et l'état de droit s'appliquent pleinement, au profit du bien-être social, de la croissance économique, de la prospérité et de l'intégrité de nos sociétés libres et démocratiques. Les gouvernements ont donc tout intérêt à travailler ensemble et à s'attaquer de conserve aux problématiques numériques. Le mécanisme du programme d'action devrait s'apparenter à une plateforme où les États pourraient dialoguer avec les parties prenantes du monde entier, y compris avec le secteur privé. Les partenariats apportent une valeur ajoutée.

La Suède défend une approche fondée sur les normes, les règles et les procédures et pratiques établies. Cependant, celles-ci sont parfois difficiles à mettre en place dans un environnement en perpétuel changement. Un excès de réglementation peut créer un décalage avec les menaces – tant actuelles que futures – ralentir voire saper l'innovation et décourager la participation des acteurs privés. Il peut aussi ne pas cadrer avec d'autres devoirs et obligations, par exemple en ce qui concerne la préservation de l'intérêt public. Le mécanisme du programme d'action doit tendre vers l'instauration d'un dialogue avec le secteur privé en matière de cybersécurité et de résilience. À cet égard, les partenariats public-privé et la participation multipartite doivent reposer sur des principes fondamentaux tels que la transparence et l'obligation de rendre des comptes, en particulier lorsqu'ils ont pour but de résoudre des problèmes concrets de politique publique.

Maintenir l'élan avant une conférence internationale en 2025

La Suède est favorable à ce que des discussions ciblées supplémentaires soient menées dans le cadre du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) afin d'étoffer le programme d'action et de trouver un consensus sur sa mise en place. Le groupe de travail devrait organiser des réunions intersessions et des sessions spéciales en 2024 et 2025, notamment pour approfondir les différents aspects du programme d'action et en rédiger le document fondateur.

La Suède est favorable à ce que de nouvelles discussions soient menées sur les modalités précises de la mise en place éventuelle d'un programme d'action, y compris dans le cadre d'une conférence internationale qui pourrait être consacrée au sujet en 2025 et à l'occasion de laquelle le document fondateur du programme d'action serait adopté sur la base des travaux préparatoires réalisés entre autres par le groupe de

travail (comme noté dans la résolution [77/37](#) de l'Assemblée générale). Cela serait l'occasion pour les parties prenantes compétentes de participer au processus (selon des modalités proches de celles adoptées dans la résolution [75/282](#) de l'Assemblée générale).

Suisse

[Original : anglais]
[14 avril 2023]

I. Introduction

1. Depuis plus de 20 ans, les États discutent, au niveau de l'ONU, des menaces existantes et potentielles liées à l'utilisation que les États font des technologies de l'information et des communications, ainsi que des moyens d'y parer. Ces discussions, qui se sont tenues dans des formats variés et limités dans le temps, ont avancé de façon considérable. Les recommandations consensuelles formulées par les groupes d'experts gouvernementaux de 2010, 2013, 2015 et 2021, celles du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale de 2021 et le rapport d'activité annuel de 2022 du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), qui fait également l'objet d'un consensus, ont bâti et consolidé un cadre de comportement responsable des États dans le cyberspace. Il prévoit l'application du droit international au cyberspace, les normes volontaires de comportement responsable des États, ainsi que des mesures de confiance et de renforcement des capacités.

2. Par le biais des résolutions [70/237](#) et [76/19](#) de l'Assemblée générale, les États Membres ont décidé par consensus que leur utilisation du numérique serait inspirée par les rapports de 2015 et 2021 des groupes d'experts gouvernementaux ainsi que par le rapport de 2021 du Groupe de travail, qui tracent les grandes lignes du cadre et entérinent les acquis.

3. La proposition de programme d'action est résolument basée sur ce cadre convenu et ses acquis.

II. Portée et objectif du programme d'action

4. Le programme d'action concourrait à la réalisation de l'objectif commun d'un cyberspace ouvert, libre, pacifique et sûr. Il offrirait une structure permanente pour la tenue d'un dialogue institutionnel régulier au niveau de l'ONU visant à aider les États Membres à mettre en place et à appliquer, à leur échelle, le cadre de comportement responsable des États dans le cyberspace.

5. Le programme d'action serait orienté vers l'action, inclusif, transparent, fondé sur le consensus et axé sur les résultats.

6. Le fait que le programme soit orienté vers l'action est essentiel, car il s'agirait d'aider les États à mettre en place des activités de coopération et de renforcement des capacités adaptées à leurs besoins. Le programme d'action fournirait une plateforme permanente de mise en commun des connaissances, des pratiques exemplaires et du savoir-faire et contribuerait ainsi à instaurer et à renforcer la confiance et la transparence.

7. Le programme d'action devrait également être assez flexible pour permettre aux États de traiter les futures menaces. Dans ce but, il devrait donner régulièrement l'occasion aux États de réexaminer le cadre et de l'étoffer, en fonction des besoins et sur la base du consensus.

III. Structure et teneur

8. Le programme d'action prévoirait la tenue annuelle d'une réunion officielle. Les États seraient invités, à titre volontaire, à dresser le bilan de leurs progrès et des difficultés rencontrées dans la mise en œuvre du cadre. Cela pourrait se faire par l'intermédiaire d'un système de soumission de rapports prévu à cet effet ou par le biais de mécanismes existants, tels que l'enquête sur l'application à l'échelle nationale des recommandations de l'Organisation des Nations Unies en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale⁵⁴. Ces évaluations offriraient l'occasion de recenser les besoins concrets et les retours d'expérience positifs, de circonscrire les problèmes et de définir les domaines prioritaires. Lors de la réunion annuelle, les États Membres adopteraient des décisions et des recommandations par consensus et formeraient les groupes de travail techniques, également par consensus.

9. Entre les sessions, les groupes de travail techniques pourraient se réunir dans les conditions fixées à la réunion annuelle. Les conclusions et les recommandations formulées seraient ensuite examinées lors de la réunion annuelle. Les domaines prioritaires abordés seraient également prédéterminés. Ils concerneraient notamment le recours à des directives concrètes et à l'échange de pratiques exemplaires pour mettre en œuvre les normes volontaires spécifiques, l'avancée des débats et de la compréhension commune de la manière dont le droit international s'applique dans le cyberspace, l'analyse des besoins en matière de renforcement des capacités et l'appui à apporter sur des questions précises.

10. Il faudrait instaurer des dialogues réguliers avec les organisations régionales et les organes internationaux compétents, comme l'Union internationale des télécommunications, pour mettre en commun les pratiques exemplaires et renforcer la coordination avec les acteurs régionaux et internationaux. Là où ces échanges ont déjà lieu, il conviendrait de mettre à profit l'expérience acquise et les structures en place, en fonction des besoins du programme d'action.

11. Une conférence d'examen pourrait se tenir de manière régulière (par exemple, tous les quatre à six ans), afin que le programme soit mis à jour en fonction des besoins.

12. Toutes les décisions prises dans le cadre du programme d'action devraient l'être par consensus.

13. Les États sont responsables au premier chef du maintien de la paix et de la sécurité internationales, y compris dans le cyberspace. Dans le même temps, l'accomplissement de leur mission ne dépend pas entièrement d'eux. C'est particulièrement vrai dans le cyberspace, où la plupart des infrastructures sont possédées et gérées par des acteurs privés. Les diverses parties prenantes jouent un rôle essentiel dans le fonctionnement du cyberspace et possèdent des connaissances et des compétences qui dépassent celles des États. C'est notamment le cas des acteurs de la société civile, du secteur privé et des milieux universitaires et techniques, qui peuvent aider les États à respecter leurs engagements pris au titre du cadre de comportement responsable dans le cyberspace. En outre, ils peuvent concourir au renforcement des capacités. Il est important que les États tirent parti de leurs compétences et de la richesse de leurs idées.

14. La prise de décision et les négociations concernant le programme d'action devraient demeurer des prérogatives des États Membres. Dans le même temps, il faudrait permettre aux diverses parties prenantes de participer et de contribuer largement et de manière substantielle aux réunions officielles annuelles, aux réunions

⁵⁴ Disponible à l'adresse suivante : <https://nationalcybersurvey.cyberpolicyportal.org/>.

d'examen et aux réunions des groupes de travail techniques. Les modalités d'organisation des réunions prévues dans le cadre du programme d'action et des réunions des groupes de travail devraient donc autoriser les parties prenantes à assister aux réunions officielles et aux sessions informelles, à faire des déclarations et à soumettre des contributions orales ou écrites à l'examen des États Membres.

IV. Travaux préparatoires et modalités d'établissement du programme d'action

15. Comme recommandé dans les rapports établis en 2021 par le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberspace dans le contexte de la sécurité internationale et par le Groupe de travail, le programme d'action devrait être étoffé, notamment dans le cadre du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Le groupe de travail actuel devrait donc y consacrer des sessions, dont il ferait figurer les conclusions dans les rapports d'activité correspondants.

16. En outre, lors de consultations menées entre les sessions, les diverses parties prenantes pourraient faire part de leurs vues et suggestions concernant la teneur et la mise en place du programme d'action.

17. La mise en place du programme d'action devrait faire l'objet d'une décision ou d'une résolution de l'Assemblée générale basée sur les travaux préparatoires réalisés entre autres par le groupe de travail. Il est possible que les États Membres demandent qu'une conférence des Nations Unies y soit consacrée.

18. Le programme d'action devrait être prêt à expiration du mandat du groupe de travail.

Tchéquie

[Original : anglais]
[14 avril 2023]

La Tchéquie apprécie les débats sur la cybersécurité à la Première Commission. Elle attache une importance particulière aux progrès réalisés dans ce domaine par le groupe de travail et le Groupe d'experts gouvernementaux, dont l'objectif est de contribuer au renforcement d'un environnement stable et pacifique en matière de numérique et, partant, de la paix et de la sécurité internationales. Les travaux de ces groupes ont permis de recenser une série de questions relatives au numérique que les États doivent examiner dans le contexte de la sécurité internationale.

Sur la base de notre analyse des travaux du Groupe d'experts gouvernementaux et du Groupe de travail à ce jour, nous pensons que le projet de programme d'action constitue un moyen approprié pour conduire systématiquement les débats sur l'utilisation du numérique dans le contexte international et de poursuivre efficacement les travaux entamés dans le cadre du Groupe d'experts gouvernementaux et du Groupe de travail. Qui plus est, un organe permanent et inclusif des Nations Unies permettrait à la communauté internationale de fixer des objectifs plus ambitieux, de soutenir leur réalisation dans le monde entier et de suivre les progrès faits de manière régulière. C'est pourquoi la Tchéquie soutient la proposition visant à mettre en place un programme d'action et en est l'un des principaux coauteurs.

Dans ce contexte, nous souhaitons contribuer aux débats sur la portée, la structure et la teneur du programme d'action en mentionnant les points suivants :

Stabilité

Selon nous, le programme d'action apporterait une stabilité institutionnelle au débat international sur le numérique. Il constituerait un cadre institutionnel permanent qui sous-tendrait tous les débats relatifs à la cybernétique à l'ONU.

- Ainsi, on éviterait des débats récurrents sur la création d'un nouveau groupe de travail consacré à l'utilisation du numérique.
- Par ailleurs, le risque de polarisation et de fragmentation des débats sur le numérique, comme on l'a vu dans le passé, en raison de l'existence parallèle malheureuse du Groupe d'experts gouvernementaux et du Groupe de travail, serait éliminé.

Inclusion et coopération public-privé

Les États sont responsables au premier chef de la sécurité internationale ; eux seuls peuvent prendre des décisions. La participation au programme d'action devrait donc être ouverte à tous les États. Les décisions prises dans le cadre du programme d'action devraient l'être par consensus.

Par ailleurs, la Tchéquie est favorable à l'ouverture des débats sur le programme d'action aux parties prenantes également. Celles-ci devraient pouvoir accéder aux groupes de travail du programme d'action, faire des déclarations et soumettre des contributions écrites.

- La participation du secteur privé, du monde universitaire et de la société civile apporterait des compétences spécialisées précieuses sur des questions telles que l'évaluation de la menace et l'application des normes, y compris la mesure des progrès accomplis.
- Le secteur privé pourrait également contribuer à l'action menée pour renforcer les capacités cybernétiques.

Mise en œuvre du cadre normatif

La Tchéquie estime que les États devraient prioriser la mise en œuvre du cadre normatif existant (approuvé par consensus dans la résolution 76/19 de l'Assemblée générale) plutôt que de le remplacer par un nouvel instrument. Dans le cadre du programme d'action, on devrait donc mettre fortement l'accent sur l'appui à la mise en œuvre du droit international existant et des normes de comportement responsable des États.

Toutefois, compte tenu de la nature singulière du numérique, il pourrait être nécessaire d'élaborer de nouvelles normes à l'avenir. Par conséquent, le programme d'action devrait être mis en place en tant qu'instrument flexible qui pourrait traiter à la fois de l'application des normes existantes et de l'élaboration possible de nouvelles normes à l'avenir.

Approfondir la compréhension de la manière dont le droit international s'applique au cyberspace

Les normes ne sont qu'un élément du cadre international de cybersécurité auquel les États doivent se conformer. Comme cela est indiqué dans les rapports finals du Groupe d'experts gouvernementaux et du premier Groupe de travail, ainsi que dans le rapport d'activité annuel du groupe de travail actuel, le droit international est applicable à l'environnement numérique et il est essentiel au maintien de la paix, de la sécurité et de la stabilité dans cet environnement. Par conséquent, le programme d'action devrait s'appuyer sur ces éléments et pourrait servir de plateforme pour

poursuivre le développement d'une position commune sur la manière dont le droit international s'applique au cyberspace.

- Dans le cadre du programme d'action, on devrait encourager les États à présenter leurs positions sur la manière dont le droit international s'applique au cyberspace et à parvenir à une position commune sur la question.
- On pourrait également tirer parti des processus multipartites existants dans ce domaine pour organiser des débats sur tel ou tel sujet dans le cadre du mandat du programme d'action, ce qui pourrait contribuer à l'application concrète d'un cadre théorique.

Soutien au renforcement des cybercapacités

Pour la Tchèque, le renforcement des cybercapacités est une priorité majeure, car il contribue à améliorer notre résilience collective mondiale face aux cyberactivités malveillantes. En d'autres termes, nous savons que le renforcement des cybercapacités a une fonction importante dans le développement mondial et que de ce fait il donne également à tous les États les moyens de participer réellement aux débats techniques et en matière de politiques sur la cybersécurité dans les instances mondiales.

- Le programme d'action serait une plateforme importante pour l'échange de vues et d'idées sur le renforcement des cybercapacités et encouragerait les activités pertinentes visant à aider les États à mettre en œuvre le cadre normatif.
- Il structurerait les initiatives de renforcement des cybercapacités en coordonnant les efforts des donateurs et en recensant les besoins des pays bénéficiaires.
- La mise en place du programme d'action nous donnerait également la possibilité d'explorer la création d'un fonds multidonateur réservé à un usage particulier, qui pourrait soutenir des activités portant exclusivement sur la promotion du cadre de comportement responsable des États.
- La coordination avec les activités de renforcement des cybercapacités menées dans d'autres enceintes, telles que l'Union internationale des télécommunications, pourrait être examinée.

Structure

En ce qui concerne les modalités spécifiques, la Tchèque penche pour des sessions plénières annuelles ou biennales et des réunions des groupes de travail techniques spécialisés durant l'intersession.

- La création et la suppression d'un groupe de travail particulier relèveraient entièrement de la compétence des États. La décision de créer ou de supprimer un groupe de travail serait prise en séance plénière par consensus.
- Les groupes de travail seraient ouverts à tous les États Membres et à toutes les parties prenantes.
- Les groupes de travail créés pour examiner diverses questions ne se réuniraient pas en parallèle, afin d'assurer une large participation.
- Ils seraient tenus de présenter des rapports d'activité.
- Ils ne se réuniraient pas uniquement à New York, mais aussi – en fonction de tel ou tel sujet – à Genève, par exemple.

Mise en place

Enfin et surtout, nous insistons sur le fait que le programme d'action ne ferait en aucune façon double emploi avec les travaux de l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

- Le programme d'action serait mis en place après que le groupe de travail actuel aura achevé ses travaux, en 2025, et s'appuierait constamment sur les travaux du groupe de travail.
- Ce serait dans le cadre du groupe de travail actuel que les États tiendraient des débats sur la forme finale que prendrait le programme d'action, notamment sur toutes les modalités nécessaires. Des sessions spéciales du groupe de travail devraient être organisées en 2024 et 2025 pour poursuivre l'élaboration des différents aspects du programme d'action, notamment du document fondateur.

En ce qui concerne la mise en place du programme d'action lui-même : selon la Tchèque, la résolution [77/37](#) de l'Assemblée générale sur la création du programme d'action indique une voie possible, à savoir l'organisation d'une conférence internationale, en supposant que la conférence adopterait le document fondateur établi par le groupe de travail.

Türkiye

[Original : anglais]
[14 mars 2023]

- Mener des études afin de réduire les écarts de maturité entre les pays en matière de cybersécurité et de méthodologie.
- Utiliser les critères de l'Indice mondial de cybersécurité de l'Union internationale des télécommunications, un indicateur essentiel reconnu du niveau de maturité des pays en matière de cybersécurité, afin de déterminer les domaines de croissance potentiels des pays en développement.
- Mesurer le niveau de maturité des équipes d'intervention informatique d'urgence en matière de détection et d'intervention pour évaluer la situation actuelle et renforcer leurs compétences.
- Améliorer l'échange de vues entre États Membres dans le cadre de l'harmonisation des règles et normes nationales avec le droit et les normes internationales.
- Encourager la coopération entre les équipes d'intervention nationales.
- Créer des canaux et des plateformes de communication d'urgence favorisant la mise en commun de ressources et d'informations entre États Membres.
- Partager pratiques exemplaires et retours d'expérience pour une meilleure compréhension des règles, des normes et des principes.
- Organiser des exercices internationaux afin de renforcer la résilience et les capacités de réaction des pays face aux cyberincidents.
- Analyser les stratégies réglementaires nationales de sécurité des technologies naissantes et préparer des guides internationaux à l'intention des membres.
- Formuler des recommandations afin de rattraper le retard accumulé en matière de renforcement des cybercapacités des pays.

- Recenser les progrès régionaux réalisés dans le renforcement des capacités nécessaires.
- Mettre en place des activités visant à améliorer les compétences du personnel chargé de la lutte contre la cybercriminalité.
- Formuler des recommandations concernant l'élaboration, l'expérimentation et le déploiement de plans d'intervention d'urgence locaux et internationaux.

Ukraine

[Original : anglais]

[14 avril 2023]

L'élaboration de mesures conjointes et concrètes visant à contrer les menaces liées à l'utilisation des technologies numériques favorisera le comportement responsable des États dans le cyberspace.

Il est de la plus haute importance de maintenir la paix, la sécurité, la coopération et la confiance internationales en ce qui concerne l'environnement numérique, en particulier à l'heure où certains États mettent au point des technologies numériques à des fins militaires et où le nombre d'incidents liés à l'utilisation malveillante de ces technologies par des acteurs étatiques et non étatiques augmente constamment.

Le programme d'action devrait servir à régler les problèmes liés à cette utilisation malveillante et à contrer les menaces qu'elle fait peser sur l'infrastructure d'information critique, sur l'infrastructure des services de base à la population, sur l'infrastructure technique nécessaire au bon fonctionnement d'un réseau Internet accessible à tous et sur le secteur de la santé.

Il faut éviter que des activités, des projets et des mesures du programme d'action fassent double emploi avec des initiatives déployées dans le cadre du groupe de travail de l'Organisation pour la sécurité et la coopération en Europe chargé du renforcement de la confiance dans le numérique.

L'Ukraine a soutenu l'adoption par consensus du premier rapport d'activité annuel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) ([A/77/275](#)) qui vise à étoffer le programme d'action, notamment dans le cadre des activités du groupe de travail.

Le programme d'action pourrait prévoir la tenue d'une ou deux réunions par an avec la participation des États, tandis que la conférence d'examen aurait lieu tous les quatre ou cinq ans. Des réunions pourraient aussi être organisées entre les sessions, et des groupes de travail seraient chargés d'étudier des questions précises.

La conférence internationale consacrée à la mise en place du programme d'action pourrait se tenir en 2025, à expiration du mandat du groupe de travail.

On pourrait envisager que les mesures nationales de mise en œuvre des règles, des normes et des principes fassent l'objet de rapports et que des réunions régulières y soient consacrées au niveau des groupes de travail.

Le programme d'action devrait prendre en compte l'importance de la coopération entre États Membres dans le domaine de la sécurité du numérique, et prévoir notamment la création de plateformes sur lesquelles on partagerait les informations concernant les vulnérabilités, les fonctions logicielles cachées et les modèles d'attaque ainsi que les résultats des analyses de sécurité des logiciels et des bibliothèques de programmes, le but étant de prévenir les attaques contre les chaînes logistiques.

Le programme d'action pourrait prévoir une procédure pour les demandes d'assistance internationale. Un mécanisme approprié existe dans le cadre du Programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous tous ses aspects.
