Nations Unies A/79/81

Assemblée générale

Distr. générale
21 mai 2024
Français
Original : anglais, chinois, espagnol, français, russe

Soixante-dix-neuvième session
Point 93 de la liste préliminaire*
Progrès de l'informatique et des télécommunications et sécurité internationale

Progrès de l'informatique et des télécommunications et sécurité internationale

Rapport du Secrétaire général

Résumé

Faisant la synthèse des communications reçues des États Membres comme suite à la résolution 78/237 de l'Assemblée générale, sans préjudice de la position de chacun d'eux sur la question, le présent rapport recense leurs vues sur la sécurité et l'utilisation des technologies de l'information et des communications, et en particulier sur le dialogue institutionnel régulier ayant trait à ces questions et organisé sous les auspices de l'Organisation des Nations Unies. Les avis reçus des États Membres dans les délais impartis sont intégralement repris dans l'annexe au présent rapport. Le rapport se conclut par les observations du Secrétaire général.

* A/79/50.

Table des matières

I. Introduction

1. Au paragraphe 8 de sa résolution 78/237, l'Assemblée générale a invité tous les États Membres à continuer d'informer le Secrétaire général de leurs vues et évaluations sur la sécurité du numérique et de son utilisation, en particulier sur le futur dialogue institutionnel régulier relatif à ces questions sous les auspices de l'Organisation des Nations Unies, et prié le Secrétaire général de lui présenter un rapport fondé sur ces vues durant sa soixante-dix-huitième session, afin que les États Membres puissent en débattre plus avant lors des réunions du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), à sa huitième session, en 2024. Le présent rapport fait suite à cette demande.

2. Le 5 janvier 2024, le Bureau des affaires de désarmement a adressé à tous les États Membres une note verbale pour appeler leur attention sur le paragraphe 8 de la résolution 78/237 et solliciter leurs vues sur la question. On trouvera à l'annexe au présent rapport les réponses reçues des États Membres au 1er mai 2024. Les points de vue reçus après cette date ont été publiés sur l'espace Réunions (Meetings Place) de la page Web du Bureau des affaires de désarmement[1].

3. On trouvera dans la partie II du présent rapport des informations générales sur les discussions engagées par les États sur la question du dialogue institutionnel régulier portant sur la sécurité et sur l'utilisation des technologies de l'information et des communications. La synthèse des communications reçues des États Membres, sans préjudice de la position de chacun d'eux sur la question, est présentées dans la partie III, la section IV étant consacrée aux conclusions et observations du Secrétaire général.

II. Contexte

4. Dans le cadre du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), les États continuent d'examiner (dans le respect de l'ordre du jour convenu du groupe de travail publié sous la cote A/AC.292/2021/1) la question de l'instauration, sous les auspices de l'ONU, d'un dialogue institutionnel régulier sur les questions connexes auquel les États participeraient largement. Au cours de sept sessions de fond du groupe de travail, de décembre 2021 à mars 2024, les États ont participé à des discussions ciblées visant à examiner plus avant les propositions relatives au dialogue institutionnel régulier, ainsi que la proposition de programme d'action.

5. Dans le deuxième rapport d'activité annuel du groupe de travail, adopté par consensus en juillet 2023 (A/78/265), les États sont convenus, en principe, que tout futur mécanisme de dialogue institutionnel régulier serait fondé sur les éléments communs suivants et ont décidé de poursuivre les discussions sur des éléments supplémentaires :

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

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

[1] https://meetings.unoda.org/ga-c1/general-assembly-first-committee-seventy-ninth-session-2024 (en anglais).

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

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

6. Les États ont aussi insisté sur l'importance du principe du consensus, tant pour la mise en place du futur mécanisme que pour ses processus décisionnels. De plus, les États étant en mesure de le faire ont été encouragés à envisager d'instaurer ou d'appuyer des programmes de parrainage et d'autres mécanismes visant à assurer une large participation aux travaux de l'ONU dans ce domaine.

7. Pendant les discussions menées dans le cadre du groupe de travail à composition non limitée sur un futur dialogue institutionnel régulier portant sur les questions liées à la sécurité du numérique, les États ont réfléchi à la portée et aux objectifs potentiels, à la structure, aux modalités (y compris pour la prise de décisions), et au suivi de la mise en œuvre. Pour faciliter les débats, le Président du groupe de travail à composition non limitée a fourni un document de travail sur les projets d'éléments relatifs à un mécanisme permanent sur la sécurité du numérique en février 2024, puis une version révisée en mai 2024. Deux réunions intersessions consacrées au dialogue institutionnel régulier ont aussi été demandées dans le cadre du deuxième rapport d'activité annuel. Lors de ces réunions, les États participeraient aussi à des discussions ciblées sur la relation entre 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 et le groupe de travail à composition non limitée[2].

III. Avis sur la sécurité du numérique et de son utilisation

Interprétations et principes généraux

8. Dans leurs communications, plusieurs États ont insisté sur la menace que représentent les activités malveillantes dans l'utilisation des technologies de l'information et des communications et noté les préoccupations internationales croissantes relatives aux menaces potentielles pour la sécurité et la stabilité internationales. Des inquiétudes ont été exprimées par un certain nombre d'États quant au développement excessif de capacités en matière de technologies de l'information et des communications à des fins incompatibles avec le droit international et avec les objectifs de maintien de la stabilité et de la sécurité internationales. Il a été constaté que certains acteurs avaient enfreint le droit international en se livrant à des activités utilisant ces technologies. Des États se sont aussi inquiétés des répercussions des activités malveillantes sur la sécurité et le bien-être des personnes.

9. Certains États ont noté que les technologies de l'information et des communications pouvaient accélérer le progrès et le développement humains, tandis que d'autres ont fait remarquer qu'elles pouvaient être utilisées à des fins incompatibles avec les objectifs de maintien de la sécurité internationale et d'une manière qui affecterait négativement le développement économique et social.

10. De nombreux États ont souligné que, compte tenu de l'environnement de sécurité actuel, il était nécessaire qu'un futur dialogue institutionnel régulier sur la

[2] Voir A/78/76.

sécurité des technologies de l'information et des communications et sur leur utilisation soit axé sur la poursuite de la promotion d'un environnement numérique ouvert, sûr, stable, accessible et pacifique. Certains États ont aussi rappelé l'importance de la coopération internationale entre les États aux fins du maintien de la stabilité internationale dans ce domaine.

11. De nombreux États ont constaté que la création d'un mécanisme permanent de prise de décision sur des questions connexes sous les auspices de l'Organisation des Nations Unies était de plus en plus demandée. De plus, nombre d'États ont souligné qu'il était essentiel de s'appuyer sur les accords conclus lors de processus antérieurs placés sous les auspices de l'Organisation, tels que les groupes d'experts gouvernementaux et le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale[3]. Certains États ont attiré l'attention sur la nécessité de s'appuyer sur cet « acquis collectif », en notant que celui-ci se compose des normes existantes relatives à l'utilisation responsable des technologies de l'information et des communications par les États, à l'applicabilité du droit international à l'utilisation de ces technologies par les États, aux mesures de confiance et au renforcement des capacités. Il a aussi été dit qu'un futur mécanisme devrait créer un espace favorisant des discussions plus approfondies sur l'application concrète des accords précédemment conclus. On a également fait valoir que le répertoire mondial et intergouvernemental d'interlocuteurs devrait faire partie intégrante de tout mécanisme futur.

12. Plusieurs États ont souligné l'importance de la continuité en ce qui concerne les résultats consensuels obtenus lors des processus précédents. Dans le même ordre d'idées, plusieurs États ont indiqué que le nouveau mécanisme institutionnel ou la nouvelle plateforme devrait être créé à l'expiration du mandat du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Certains États ont fait ressortir que cela devrait être fait au plus tard en 2026, pour assurer la continuité.

13. Plusieurs États ont insisté sur l'importance d'éviter toute duplication des efforts internationaux déployés dans ce domaine et mis en garde contre la poursuite de processus parallèles, en évoquant les problèmes de capacité qui en découlent pour les délégations. De nombreux États ont souligné l'importance d'un dialogue institutionnel unique, permanent et inclusif, mené régulièrement, sous les auspices de l'Organisation des Nations Unies. Certains États ont noté que la mise en place d'un mécanisme unique, inclusif et permanent contribuerait également à la prévisibilité et à la stabilité institutionnelles, tout en évitant de devoir négocier de nouveaux mandats à intervalles réguliers. Il a aussi été constaté que les petits États et les États en développement disposant de ressources limitées ne seraient pas en mesure de participer durablement à des processus parallèles doubles. De plus, on a également estimé qu'un futur mécanisme devrait servir de point d'entrée unique pour le traitement de la question de la sécurité des technologies de l'information et des communications.

14. Par ailleurs, certains États ont réaffirmé que le droit international, en particulier la Charte des Nations Unies, était applicable et essentiel au maintien de la paix, de la sécurité et de la stabilité dans l'environnement numérique. À cet égard, il a été dit que des discussions plus approfondies sur la manière dont le droit international s'applique pourraient avoir lieu dans le cadre d'un futur mécanisme. Il a été suggéré d'étudier la possibilité de créer un groupe de travail sur cette question dans le cadre d'un futur mécanisme. Certains États ont estimé que ce mécanisme pourrait servir de

[3] Voir A/65/201, A/68/98, A/70/174, A/75/816 et A/76/135.

cadre inclusif pour les discussions sur le droit international, y compris pour la mise en commun des opinions nationales, l'organisation de réunions d'experts et l'exploration des activités de renforcement des capacités dans ce domaine.

15. Les États ont réfléchi à plusieurs principes fondamentaux qui devraient servir de socle à tout futur mécanisme de dialogue institutionnel régulier sur la sécurité et l'utilisation des technologies de l'information et des communications (tels que l'ouverture, l'inclusivité et la transparence), et au fait qu'un tel mécanisme devrait être pragmatique, unique et démocratique. On a estimé que le futur mécanisme devrait être dirigé par les États et s'appuyer sur le respect des principes de la Charte, tels que l'égalité souveraine des États, le non-recours à la menace ou à l'emploi de la force et le règlement pacifique des différends. Il a aussi été suggéré qu'il devrait permettre une certaine souplesse et un développement évolutif en fonction de la progression des besoins des États et de l'apparition de nouvelles tâches liées à la sécurité dans l'utilisation des technologies numériques.

16. Plusieurs États ont évoqué la proposition de programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale. Il a été noté que cette proposition avait été citée dans les rapports précédents présentés par les organes concernés de l'Organisation des Nations Unies, et notamment dans les rapports annuels du groupe de travail à composition non limitée adoptés par consensus. Il a aussi été relevé que la proposition avait été soutenue par un groupe interrégional d'États et qu'elle pourrait servir de structure permanente pour les débats sur les technologies de l'information et des communications dans le contexte de la sécurité internationale, après l'expiration du mandat de l'actuel groupe de travail à composition non limitée.

17. Plusieurs États ont indiqué qu'un groupe de travail permanent à composition non limitée devrait être créé immédiatement après la fin du mandat actuel, qui court jusqu'en 2025. Ces États ont noté que l'actuel groupe de travail à composition non limitée avait prouvé par son efficacité et son utilité que ce format était le meilleur pour un tel mécanisme et pour un groupe de travail décisionnel permanent à composition non limitée chargé d'axer ses travaux sur la poursuite de la promotion d'un environnement numérique ouvert, sûr, stable, accessible et pacifique, notamment par l'élaboration de règles, de normes et de principes juridiquement contraignants relatifs au comportement responsable des États et par la création d'un mécanisme efficace pour leur application, en tant qu'éléments d'un futur traité universel visant à garantir la sécurité internationale de l'information.

Portée et objectifs

18. De nombreux États ont souligné que le principal objectif d'un futur dialogue institutionnel régulier sur la sécurité du numérique et son utilisation était de contribuer à la paix et à la sécurité internationales dans ce domaine. Plusieurs États ont rappelé que tout mécanisme futur devrait promouvoir un environnement numérique ouvert, sûr, stable, accessible et pacifique. Certains États ont aussi relevé qu'un tel mécanisme devrait faciliter le dialogue et la coopération entre les États et contribuer à la prévention des conflits et des malentendus.

19. Plusieurs États ont souligné que les recommandations par consensus adoptées au titre des processus précédemment créés dans le cadre de l'Organisation des Nations Unies, qui ont abouti à un cadre consolidé de comportement responsable des États dans l'utilisation des technologies numériques, devraient rester au cœur de tout futur mécanisme institutionnel. Plusieurs États ont souligné qu'il importait d'appuyer la mise en œuvre des résultats précédemment arrêtés, tandis que d'autres ont noté qu'un futur mécanisme devrait envisager la mise en œuvre pratique des accords conclus par

le groupe de travail à composition non limitée. Il a été suggéré qu'un futur mécanisme pourrait élaborer des orientations concrètes pour aider les États à appliquer le cadre normatif convenu, ainsi que pour améliorer la compréhension du cadre lui-même.

20. Dans leurs contributions, les États ont réfléchi à la nécessité de développer davantage le cadre existant. Certains États ont indiqué qu'il était possible de recenser les lacunes existantes, d'élaborer des normes supplémentaires ou de formuler de nouvelles règles et obligations juridiquement contraignantes. Plusieurs États se sont prononcés en faveur d'un instrument juridiquement contraignant, tandis que d'autres ont souligné que le cadre pourrait être développé et mis à jour, si nécessaire, en réponse à de nouvelles menaces évoluant au fil du temps. Plusieurs États ont noté que le mécanisme devrait trouver un équilibre entre deux activités d'égale importance : la mise en œuvre du cadre établi et son développement ultérieur.

21. Il a été dit qu'un futur mécanisme devrait tenir compte du passé et de l'avenir afin de cibler à la fois l'observation et la mise en œuvre du cadre convenu de comportement responsable des États dans l'utilisation des technologies numériques, et en particulier l'enrichissement du renforcement des capacités, l'élaboration de nouvelles normes compte tenu de l'évolution de la situation (sur la sécurité des données, par exemple), la création de nouveaux plans d'action portant sur le renforcement des capacités, et un instrument juridiquement contraignant.

22. De nombreux États ont fait ressortir que la question du renforcement des capacités devrait occuper une place centrale dans tout futur mécanisme. Certains ont souligné qu'il importait de créer des synergies entre les activités existantes, notamment les initiatives connexes de l'Union internationale des télécommunications et de la Banque mondiale. On a aussi évoqué les principes convenus en matière de renforcement des capacités figurant en annexe du deuxième rapport d'activité annuel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025)[4]. Plusieurs États ont noté qu'un futur mécanisme devrait faciliter les efforts de renforcement des capacités, notamment par l'échange d'informations sur les meilleures pratiques. Plusieurs États ont rappelé qu'il fallait mener des activités ciblées et fondées sur les besoins. Il a été avancé que la fonction de renforcement des capacités d'un mécanisme doit être directement liée aux efforts déployés par les États au niveau national pour mettre en œuvre le cadre normatif de comportement responsable de l'État.

23. Par ailleurs, la possibilité de créer un mécanisme de financement propre, utilisant l'expérience des mécanismes existants dans d'autres instances de l'ONU dans le but de soutenir les efforts de renforcement des capacités, a aussi été évoquée. Il a été suggéré de mettre en place un système de partenariat interrégional volontaire, dans le cadre duquel des États aux capacités diverses pourraient être mis en relation afin de renforcer la coopération et d'échanger des bonnes pratiques. Il a été proposé d'instaurer un mécanisme de renforcement des capacités à plusieurs composantes, qui comprendrait des échanges sur l'évolution des menaces, le recensement par chaque pays des besoins en matière de capacités et l'adéquation entre les besoins et les ressources, ainsi qu'un dispositif permettant de formuler des commentaires aux fins d'échanges d'expériences connexes.

24. Plusieurs États ont noté qu'un futur mécanisme pourrait servir de cadre institutionnel d'ensemble pour les initiatives et les efforts connexes dans le domaine de la sécurité des technologies de l'information et des communications, y compris le répertoire mondial et intergouvernemental d'interlocuteurs.

[4] A/78/265, annexe C.

25. D'autres domaines d'action potentiels ont été suggérés par les États, notamment la définition d'une vision commune de la manière dont le droit international s'applique à l'utilisation des technologies numériques et dont les normes existantes peuvent être adaptées aux caractéristiques propres au domaine. Il a été dit qu'un futur mécanisme pourrait faire progresser les discussions sur les menaces existantes et émergentes et sur la manière dont le droit international, y compris le droit international humanitaire et les droits humains, s'applique à l'utilisation des technologies de l'information et des communications par les États. L'élaboration et l'application de mesures de confiance et de mécanismes de coopération pratique entre les États ont aussi été considérées comme des points devant être traités.

Établissement, modalités et prise de décision

26. Les États ont mené différentes réflexions sur les modalités de mise en place d'un futur mécanisme, et sur les activités préparatoires nécessaires. Il a été estimé que les contributions soumises par les États Membres dans le cadre de l'actuel groupe de travail à composition non limitée (portant notamment sur la proposition de programme d'action), le rapport du Secrétaire général sur ce programme d'action (établi comme suite à la résolution 77/37), le présent rapport[5], et les recommandations applicables formulées dans les rapports de l'actuel groupe de travail à composition non limitée, devraient constituer la base de la création du futur mécanisme en ce qui concerne son champ d'application, sa structure et ses modalités.

27. De nombreux États ont souligné qu'il importait de parvenir à un consensus sur le champ d'application, la structure et les modalités du futur mécanisme. De nombreux États se sont déclarés favorables à la poursuite de l'élaboration et du développement du mécanisme dans le cadre de l'actuel groupe de travail à composition non limitée. Plusieurs États ont souscrit à la poursuite de discussions ciblées et approfondies dans le cadre de l'actuel groupe de travail à composition non limitée afin d'élaborer le mécanisme et de parvenir à un consensus sur son format et sa structure. En ce qui concerne le programme d'action, plusieurs États ont soutenu la tenue de réunions intersessions consacrées à cette proposition en 2024 et 2025 afin de mettre au point d'autres aspects du mécanisme. Des discussions plus approfondies sur les implications budgétaires ont aussi été suggérées.

28. On a pris note de la possibilité d'établir un futur dialogue institutionnel régulier via une résolution de consensus de l'Assemblée générale. À cet égard, il a été dit qu'une résolution de l'Assemblée générale devrait créer un groupe de travail permanent à composition non limitée. On a aussi fait valoir que l'actuel groupe de travail à composition non limitée pourrait établir le futur mécanisme au moyen d'une déclaration politique qui serait ensuite approuvée par l'Assemblée générale. Il a été suggéré que l'affirmation de l'engagement pris par les États au titre du cadre de comportement responsable des États pourrait constituer un élément clé d'une telle déclaration politique.

29. En ce qui concerne la proposition de programme d'action, plusieurs États ont indiqué qu'ils étaient favorables à la création d'un tel programme au moyen d'une déclaration politique. Il a été suggéré que cette déclaration pourrait être complétée par une résolution de la Première Commission qui décrirait les tâches, la structure et les modalités dudit programme, et qu'une conférence internationale pourrait être convoquée, au plus tard en 2026, afin d'élaborer et d'adopter une telle déclaration. Il a été dit que, si le groupe de travail à composition non limitée actuel ne parvenait pas à un consensus sur un rapport final (et notamment à un accord sur un mécanisme), une conférence internationale plus complète ou un autre processus préparatoire créé

[5] A/78/76.

par l'Assemblée générale serait nécessaire pour assurer la continuité de ces importantes discussions multilatérales.

Mécanisme de suivi et mise en œuvre

30. Les États ont formulé diverses suggestions relatives au mécanisme de suivi, notamment des réunions régulières, telles que des réunions plénières et des conférences d'examen, ainsi que des réunions intersessions, y compris des groupes de travail techniques. Il a aussi été proposé d'organiser des réunions formelles annuelles du mécanisme. Les propositions relatives à la fréquence des réunions plénières varient de tous les deux ans à tous les trois ans. On a estimé que le futur mécanisme devrait convoquer des réunions biennales pour exécuter le programme de travail arrêté. On a aussi jugé qu'il pourrait être utile de réexaminer périodiquement le fonctionnement du mécanisme permanent afin de s'assurer que ses travaux sont adaptés à l'évolution constante des menaces opérationnelles.

31. Certains États ont soutenu la création de groupes de travail techniques chargés de se concentrer sur des questions prioritaires précises, telles que l'applicabilité du droit international et l'élaboration de nouvelles normes, règles et principes, ainsi que d'obligations juridiquement contraignantes, le cas échéant. Il a aussi été dit que les groupes de travail techniques constitueraient l'essence d'un mécanisme pragmatique. Il a été proposé que des sous-groupes subsidiaires examinent des aspects précis du mandat du mécanisme. Il a été avancé que les réunions des groupes de travail techniques portant sur des questions précises et organisées pendant la période intersessions devraient se tenir dans un format hybride pour faciliter une large participation des États. Il a été noté que les réunions des sous-groupes ne devraient pas se tenir en parallèle afin d'assurer la pleine participation des délégations. Enfin, il a été suggéré de créer un programme de bourses pour faciliter une large participation des États.

32. Les États ont proposé différentes périodicités pour les conférences d'examen potentielles, notamment tous les trois, quatre ou six ans. Certains États ont noté que lors de ces conférences, on devrait passer en revue le cadre de comportement responsable des États, afin de le mettre à jour si nécessaire et de donner une orientation stratégique aux travaux du mécanisme. Il a été observé que les conférences d'examen devraient déterminer s'il était nécessaire d'élaborer des normes, règles, principes ou obligations contraignantes supplémentaires sur la base du consensus.

33. De nombreux États ont souligné l'importance de la prise de décision par consensus dans le cadre d'un futur mécanisme. Certains ont souligné que les décisions sur les questions de fond devaient être prises par consensus. Plusieurs États ont estimé que le principe de décisions prises par consensus exclusivement par les États devrait être clairement énoncé dans le document établissant le futur mécanisme. Les États ont suggéré diverses formes de consolidation des décisions prises par les États dans le cadre d'un futur mécanisme, telles que des rapports d'activité présentés à l'Assemblée générale tous les deux ans et des rapports de procédure annuels accompagnés des décisions consensuelles connexes.

34. Certains États ont évoqué la possibilité d'établir des rapports nationaux volontaires dans le cadre d'un futur mécanisme. Il a été suggéré d'établir des rapports sur la mise en œuvre nationale du cadre normatif, ainsi que sur les pratiques nationales. On a aussi proposé d'utiliser des outils 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 et de l'Organisation des Nations Unies[6].

35. Plusieurs États ont noté que si la prise de décision restait la prérogative exclusive des États, les échanges avec les organisations régionales et sous-régionales pourraient être bénéfiques, notamment pour tirer parti des synergies et s'appuyer sur les structures et les plateformes de renforcement des capacités existantes. Il a été suggéré d'organiser chaque année des réunions intersessions avec les représentants de ces organisations, sur la base de consultations avec des groupes de pays et la présidence du futur mécanisme. Il a aussi été proposé d'échanger les meilleures pratiques aux niveaux international, interrégional et régional.

36. Les États ont diversement réfléchi au dialogue avec des entités non gouvernementales dans le cadre d'un futur mécanisme, en citant en exemple les modalités de participation à d'autres forums de l'Organisation des Nations Unies, tels que 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 et le Groupe de travail à composition non limitée sur le vieillissement. De nombreux États ont indiqué que la participation de plusieurs parties prenantes était importante pour le fonctionnement futur du mécanisme. Il a été noté que la participation de toutes les parties prenantes au futur dialogue institutionnel régulier contribuerait à la réalisation de l'objectif commun de maintien de la paix et de la sécurité dans le domaine du numérique et pourrait apporter une expertise précieuse sur des questions telles que l'évaluation des menaces et l'application des normes. Certains États ont soutenu la participation d'entités non gouvernementales conformément aux modalités convenues dans l'actuel groupe de travail à composition non limitée. Plusieurs États ont déclaré être favorables à la participation formelle des parties intéressantes et au fait qu'elles soient consultées régulièrement, tandis que d'autres ont estimé que le dialogue avec les acteurs non étatiques devrait être strictement consultatif et informel, par exemple dans le cadre de réunions intersessions annuelles.

37. Certains États ont désigné le Bureau des affaires de désarmement comme l'entité appropriée pour assurer le secrétariat d'un futur mécanisme.

IV. Observations et conclusions du Secrétaire général

38. Il faut de toute urgence préserver la paix et la sécurité de l'environnement numérique. Alors que les inquiétudes suscitées par l'utilisation malveillante de ces technologies par toute une série d'acteurs vont croissant, la communauté internationale doit faire face à une fracture numérique grandissante et à une échéance qui se rapproche rapidement pour la réalisation des objectifs de développement durable. Il est impératif de prendre des mesures concrètes pour empêcher que les conflits ne se propagent et ne se poursuivent dans ce domaine, et notamment pour protéger les vies humaines des activités malveillantes.

39. La communauté internationale doit relever de formidables défis pour maintenir la paix et la stabilité dans le domaine des technologies de l'information et des communications, mais elle dispose d'une base solide sur laquelle elle peut s'appuyer. Depuis plus de vingt ans, grâce à des processus menés sous les auspices de l'Assemblée générale, les États ont accompli des progrès décisifs dans la détection des menaces existantes et émergentes, dans l'analyse de l'applicabilité du droit international à l'utilisation des technologies de l'information et des communications par les États, dans l'élaboration d'un cadre de comportement responsable des États

[6] https://nationalcybersurvey.cyberpolicyportal.org (en anglais).

dans l'utilisation de ces technologies, et dans l'examen des mesures de confiance et des initiatives de renforcement des capacités. Ces progrès cumulés et cohérents ont été réalisés sur la base d'accords de consensus, qui forment une base solide pour les progrès à venir.

40. Les efforts entrepris par les États dans le cadre du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) montrent qu'il est possible d'adopter de nouvelles mesures concrètes pour atteindre l'objectif commun, à savoir un environnement pacifique et sûr en matière de technologies numériques. Les progrès constants réalisés dans ce groupe prouvent que lorsque la volonté politique est suffisante, il est possible non seulement de parvenir à des accords communs mais aussi de mener une action concrète. À cet égard, je me félicite du consensus auquel sont parvenus les États aux fins de la création d'un répertoire mondial et intergouvernemental d'interlocuteurs afin de renforcer les échanges et la coopération entre eux. Il s'agit d'une mesure significative qui favorise la paix et la sécurité internationales et renforce la transparence et la prévisibilité.

41. Dans ce contexte, les États ont reconnu qu'il était crucial de maintenir un dialogue institutionnel régulier sur ces questions afin de disposer d'un espace suffisant pour réaliser des progrès continus. Ces questions seront de plus en plus d'actualité à mesure que ces technologies deviendront toujours plus omniprésentes et feront partie intégrante de notre vie quotidienne.

42. Les États s'accordent généralement à dire que l'Organisation des Nations Unies est le meilleur espace pour accueillir un tel dialogue institutionnel régulier, dans la mesure où il s'agit d'une plateforme pleinement inclusive. Il est communément admis qu'un tel dialogue institutionnel soutient les objectifs communs de renforcement de la paix et de la stabilité internationales et de prévention des conflits dans l'environnement numérique. Les États affirment aussi plusieurs principes essentiels sur lesquels reposerait un tel dialogue, par exemple l'inclusivité, la transparence et une approche pragmatique. De plus, tous reconnaissent la nécessité d'un mécanisme unique qui facilite la participation la plus large possible des États.

43. Compte tenu de ces larges convergences de vues et de ces opinions générales, il semble possible de parvenir à un consensus sur un futur dialogue institutionnel régulier sur les technologies de l'information et des communications dans le contexte de la sécurité internationale. Compte tenu des succès déjà obtenus, les États disposent d'une excellente occasion, dans le cadre du groupe de travail à composition non limitée, de trouver un terrain d'entente sur un mécanisme permanent unique, placé sous les auspices de l'Organisation des Nations Unies, qui fonctionnerait de manière ouverte, inclusive et transparente. Les éléments communs pour un futur dialogue institutionnel régulier établis par consensus dans le rapport d'activité annuel de 2023 du groupe de travail à composition non limitée constituent un point de départ logique et utile. Ces questions sont trop importantes pour ne pas saisir cette occasion de renforcer la confiance. La prochaine phase logique de l'examen multilatéral de ces questions est d'aborder la question d'un mécanisme permanent placé sous les auspices de l'Organisation des Nations Unies, en faisant fond des succès passés et en préparant le terrain pour les progrès futurs.

Annexe

Réponses reçues des gouvernements

Allemagne

[Original : anglais]
[30 avril 2024]

A. Principes fondamentaux du programme d'action

L'Allemagne préconise la mise en place d'un programme d'action qui doterait la Première Commission d'un mécanisme permanent, transparent, 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 serait 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 deviendrait opérationnel au plus tard en 2026 pour donner suite aux conclusions du groupe de travail après l'achèvement de son mandat, conformément à la résolution 78/16 de l'Assemblée générale, dans laquelle celle-ci a décidé de créer un mécanisme placé sous l'égide de l'Organisation des Nations Unies, qui aurait pour objectifs ceux énoncés dans la résolution 78/37 et les éléments communs établis par consensus dans le deuxième rapport annuel d'activité du groupe de travail à composition non limitée (2021-2025) (A/78/265).

Il convient d'éviter les mécanismes parallèles ou les doubles structures afin de ne pas surcharger les États, qui ne seraient pas en mesure d'y participer de manière constructive, et de garantir des débats orientés vers l'action. Les discussions menées entre les États sur la portée, la structure et la teneur du programme d'action doivent se poursuivre au sein de l'actuel groupe de travail à composition non limitée 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 cyberespace en facilitant le dialogue et la coopération entre les États pour mettre en œuvre le cadre international visant à 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 aux principes convenues en matière de renforcement des capacités énoncés dans l'annexe C du deuxième rapport d'activité annuel. Tirer parti des synergies avec les mécanismes prévus par d'autres instances afin d'éviter les structures faisant double emploi et l'éparpillement des ressources.
- Mettre en œuvre des mesures de confiance, notamment celles recensées dans la première liste non exhaustive de mesures de confiance approuvée dans le deuxième rapport d'activité annuel (A/78/265, annexe B), en particulier pour ce qui est du 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 progresser les débats 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. Il devrait permettre de poursuivre les discussions et, le cas échéant, de développer le cadre international de comportement responsable des États dans le cyberespace afin de l'adapter 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. Fonction, 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.

Compte tenu des éléments communs établis par consensus dans le deuxième rapport d'activité annuel, 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 cyberespace ;

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 a été établi par l'actuel groupe de travail à composition non limitée. Le répertoire, qui constitue lui-même une mesure de confiance, devrait aussi définir le cadre de mise en œuvre de la liste globale non-exhaustive de mesures de confiance qui figure dans le deuxième rapport d'activité annuel, l'objectif général étant de réduire le risque de malentendus et de conflits dans le cyberespace. Il conviendrait également de s'en servir pour examiner, adopter et mettre en œuvre d'autres mesures de confiance au niveau mondial. En facilitant l'élaboration et l'application de mesures de confiance adaptées, le répertoire constituerait un pilier central du programme d'action, qui met l'accent sur la mise en œuvre du cadre existant ;

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

d) 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 ;

e) 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, établies par consensus dans le deuxième rapport d'activité annuel) et mène des activités de recherche liées à la mise en œuvre du cadre ;

f) 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 de participer de manière véritable 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.

Les États conserveront le droit exclusif de négocier les textes convenus et de prendre des décisions dans le cadre du programme d'action. Celui-ci devrait également prévoir des mécanismes de dialogue avec les parties prenantes non gouvernementales (organisations multilatérales et régionales, société civile, secteur privé et universités). Il devrait offrir aux parties prenantes des possibilités de participation inclusive et véritables 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, des conférences d'examen et des réunions supplémentaires des groupes de travail techniques organisées entre les sessions. La majorité des instances devrait en outre proposer des modalités de participation hybrides afin 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 de comportement responsable des États dans le cyberespace 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]
[1er mai 2024]

En réponse à l'invitation formulée par l'Assemblée générale dans sa résolution 78/237, l'Australie se félicite de l'occasion qui lui est donnée de présenter ses vues sur la promotion du comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et de poursuivre le dialogue mené au niveau international.

La présente communication se fonde sur les contributions envoyées par l'Australie en réponse aux résolutions 77/37, 76/19, 75/32, 74/28, 70/237, 68/243 et 65/41 sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale adoptées en 2023, 2022, 2021, 2020, 2016, 2014 et 2011, respectivement.

Stratégie australienne de cybersécurité pour la période 2023-2030

Le 22 novembre 2023, Clare O'Neil, la Ministre de la cybersécurité, a lancé la stratégie australienne de cybersécurité pour la période 2023-2030, qui définit la vision de l'Australie en matière de cybersécurité nationale et internationale et repose sur une approche nationale visant à renforcer la cyberrésilience.

La stratégie recense six boucliers permettant de renforcer les cyberdéfenses et de rebondir rapidement après un cyberincident : a) des entreprises et des citoyens forts ; b) des technologies sûres ; c) le partage et le blocage des menaces à l'échelle mondiale ; d) la protection des infrastructures critiques ; e) les capacités souveraines ; f) un leadership régional et mondial résilient.

La stratégie définit l'engagement continu de l'Australie en faveur de l'élaboration, de l'application et de la défense des règles, normes et standards internationaux cyber, notamment par le respect du droit international et des normes de comportement responsable des États dans le cyberespace, et par le déploiement de toutes les armes dont dispose l'État pour dissuader les acteurs malveillants et faire face à leurs agissements.

Respect du droit international et des normes de comportement responsable des États dans le cyberespace

L'Australie collaborera avec ses partenaires actuels et établira de nouveaux partenariats pour faire respecter le droit international et le cadre convenu pour un comportement responsable des États, sur lequel reposent notre stabilité, notre prospérité, notre indépendance et notre souveraineté dans le cyberespace.

Tous les pays se sont mis d'accord sur un cyberespace réglementé, fondé sur le droit et les normes internationaux existants. Le droit international, que viennent compléter des normes volontaires convenues relatives au comportement responsable des États, les mesures de confiance et le renforcement des capacités, fournit un cadre solide aux fins de la prévisibilité et de la stabilité dans le cyberespace. Si le Cadre est appliqué et respecté, il contribue à faire face aux menaces que représente la cyberactivité malveillante provoquée ou parrainée par des États.

L'Australie œuvrera de concert avec ses partenaires internationaux dans le cadre des échanges organisés sous les auspices de l'Organisation des Nations Unies afin de clarifier l'application du droit international au cyberespace et de renforcer la mise en œuvre du cadre de comportement responsable des États dans le cyberespace. Ces efforts consisteront notamment à renforcer la coopération au moyen de forums régionaux, notamment dans le cadre du Forum des îles du Pacifique et par la participation au Forum régional de l'Association des nations de l'Asie du Sud-Est.

Déployer toutes les armes dont dispose l'État pour dissuader les acteurs malveillants et réagir à leurs agissements

L'Australie déploiera toutes les armes dont dispose l'État pour dissuader les cyberacteurs malveillants et réagir à leurs agissements. Elle collaborera avec ses partenaires internationaux pour prendre des mesures visant à faire payer les personnes et les organisations qui rendent le cyberespace moins sûr. Il s'agit notamment d'attirer l'attention sur les cas où les États agissent en violation du droit et des normes internationaux, et d'imposer des sanctions à ceux qui commettent ou facilitent des cyberincidents de grande ampleur, lorsqu'elle dispose de preuves suffisantes et qu'il est dans son intérêt national de le faire.

Dans toutes ses actions, l'Australie respectera le droit international existant et les normes volontaires convenues en matière de comportement responsable des États dans le cyberespace.

Soutenir une région cyberrésiliente

L'Australie continuera de collaborer avec ses voisins du Pacifique et de l'Asie du Sud-Est pour construire une région plus cyberrésiliente. Ses activités de coopération et d'assistance continueront d'être coordonnées par l'Ambassadeur chargé des affaires cyber et des technologies critiques.

L'Australie recentre ses efforts en matière de coopération et de renforcement des capacités dans le domaine cyber afin qu'ils soient plus ciblés, plus efficaces et plus durables, et qu'ils permettent à ses voisins de mieux prévenir les cyberincidents et de s'en remettre rapidement lorsqu'ils se produisent. Conscient que le public

s'intéresse aux questions de cybersécurité de différentes manières, elle continuera de prendre en compte l'égalité des genres, le handicap et l'inclusion sociale. Il s'agit notamment de continuer d'appuyer les priorités concernant les femmes et la paix et la sécurité de l'Organisation des Nations Unies, ainsi que le Plan d'action national australien sur les femmes, la paix et la sécurité (2021-2031).

Lorsque des cyberincidents graves se produiront dans sa région, l'Australie sera mieux placée pour répondre aux demandes d'assistance. Elle est en train de mettre en place une équipe régionale de réponse aux cybercrises au Ministère des affaires étrangères et du commerce, qui s'appuiera sur l'expertise du gouvernement, du secteur et de la communauté technique. En réponse aux demandes des gouvernements à la suite de cyberincidents importants dans la région, cette équipe aidera à contenir la propagation et les répercussions des cyberincidents et à rétablir les services et infrastructures critiques.

Dialogue institutionnel régulier

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'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 cyberespace, 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 a pour objectif général de contribuer à la paix et à la sécurité internationales dans le cyberespace 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.

Dans sa résolution 77/37, l'Assemblée générale a accueilli favorablement la proposition d'établir le programme d'action et a prié le Secrétaire général de solliciter les vues des États Membres sur la portée, la structure et la teneur du programme d'action. Dans ce rapport (A/78/76), il a été 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 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.

Le groupe de travail à composition non limitée joue un rôle clé dans l'élaboration du programme d'action et les travaux préparatoires connexes. Le programme d'action devrait s'appuyer sur les avancées consensuelles obtenues de haute lutte et sur les discussions cumulées des six derniers groupes successifs d'experts gouvernementaux et des groupes de travail inaugural et actuel à composition non limitée. La phase suivante ou l'évolution de la cyberarchitecture de l'Organisation des Nations Unies prendrait la forme d'un mécanisme permanent, 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.

Dans sa résolution 78/16, l'Assemblée générale a décidé de créer, à l'issue des travaux du groupe de travail à composition non limitée (2021-2025) et au plus tard en 2026, un mécanisme placé sous l'égide de l'Organisation des Nations Unies, lequel sera permanent, inclusif et orienté vers l'action et aura pour objectifs ceux énoncés dans sa résolution 77/37 et les éléments communs pour un futur dialogue institutionnel régulier établis par consensus dans le rapport d'activité annuel de 2023 du groupe de travail à composition non limitée (2021-2025).

L'Australie soutient la proposition de tenir une conférence internationale en 2025, afin d'adopter le document fondateur du programme d'action, sur la base des travaux préparatoires réalisés dans le cadre du groupe de travail à composition non limitée (2021-2025).

L'Australie est favorable à un document fondateur énonçant les engagements des États et prévoyant un mécanisme qui pourrait être approuvé dans le cadre d'une résolution de l'Assemblée générale. Ce document fondateur, qui pourrait prendre la forme d'une 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 cyberespace), comme convenu dans les rapports successifs du Groupe d'experts gouvernementaux[7] 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 internationale[8].
- 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 à composition non limitée.
- 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, 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, en fonction des 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.

En ce qui concerne le règlement intérieur, 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).

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

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

d'un renforcement des capacités adapté, 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/, en anglais).

L'Australie est consciente de l'importance de la communauté multipartite, notamment la société civile, le secteur privé, le monde universitaire et la communauté technique, pour ce qui est de contribuer à un cyberespace gratuit, ouvert, sûr, stable, accessible et pacifique. De plus, elle propose que le programme d'action prévoie une consultation régulière et institutionnalisée des parties prenantes concernées.

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.

L'Australie attend 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.

Azerbaïdjan

[Original : anglais]
[1er mai 2024]

Au cours des dernières années, le cyberespace a considérablement évolué, et offre désormais des perspectives d'amélioration de notre vie quotidienne, de la sûreté et de la sécurité à la vitesse de communication et à l'utilisation des technologies numériques. Les progrès réalisés dans le domaine des technologies cyber et critiques sont le fondement de la prospérité future du monde, mais ils peuvent aussi nuire à la stabilité et à la prévisibilité. Il est donc essentiel d'encourager les mesures de renforcement des capacités, les capacités de protection adéquates et les services numériques qui contribueront à rendre le cyberespace plus sûr.

Efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine

L'Azerbaïdjan appuie les travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), créé par la résolution 75/240 de l'Assemblée générale. Le pays est l'un des coauteurs de la résolution 78/237 et a adopté plusieurs mesures pour renforcer sa sécurité informatique et promouvoir la coopération internationale en matière de cybersécurité.

Il faut noter que la stratégie de la République d'Azerbaïdjan sur la sécurité de l'information et la cybersécurité pour la période 2023-2027, approuvée par le décret présidentiel du 28 août 2023, vise à renforcer le niveau national de sécurité de l'information aux fins d'une utilisation sécurisée des technologies modernes de l'information et des communications par l'État, la société et les personnes, ce qui implique la mise au jour et l'application de mesures visant à garantir la sécurité de l'État, des réseaux privés et des infrastructures d'information critiques, ainsi que la protection des données personnelles, et contribue ainsi à la création de conditions plus favorables au respect des droits humains et des libertés qui sont inscrits dans la Constitution de la République d'Azerbaïdjan. Première stratégie adoptée en matière de sécurité de l'information et de cybersécurité en République d'Azerbaïdjan, elle fait partie intégrante de la politique de l'État en matière de technologies de l'information et des communications et présente ses principaux objectifs, orientations, tâches prioritaires, solutions respectives et un plan de mesures globales dans ce domaine.

De plus, dans le plan d'action de la stratégie, au point 8.9.2.3, il est fait mention d'une mesure continue visant à organiser le développement de la coopération internationale et l'étude de l'expérience internationale en matière de cybersécurité au niveau des entités chargées de la sécurité de l'information, dont l'équipe nationale d'intervention en cas d'urgence informatique et d'autres équipes d'intervention en cas d'urgence informatique, l'objectif principal étant le développement de la coopération avec les centres internationaux d'équipes d'intervention informatique d'urgence et l'adhésion à ces centres. Des travaux pratiques sont actuellement menés en vue de développer les activités mutuelles et l'échange d'expériences.

Il convient de noter que les règles visant à assurer la sécurité des infrastructures d'information critiques dans la République d'Azerbaïdjan et les règles portant sur la structure, la création et la gestion du registre des objets d'infrastructure d'information critiques ont été approuvées par des décisions du Conseil des ministres de la République d'Azerbaïdjan en 2023.

De plus, grâce aux mesures conjointes prises par le Service de sécurité de l'État et l'Association des organisations de cybersécurité d'Azerbaïdjan, le pays est passé de la quatre-vingt-sixième à la cinquantième place dans le tableau de classement international de l'indice national de cybersécurité en 2023.

Le Service d'État chargé des communications spéciales et de la sécurité de l'information a élaboré un projet de lignes directrices, qui sera présenté aux agences gouvernementales et vise à garantir la sécurité de l'information dans les institutions de l'État, y compris par la mise au jour des mesures préventives et correctives contre les menaces potentielles dans les environnements d'information des entreprises.

Un projet de cyberhygiène a été déployé pour renforcer la cyberrésilience face aux cybermenaces et sensibiliser les employés des institutions publiques, ainsi que le secteur privé et les chefs d'entreprise.

Un cyberfestival, le Critical Infrastructure Defense Challenge 2023, organisé conjointement par le Service d'État pour les communications spéciales et la sécurité de l'information et le Service de sécurité de l'État, s'est tenu les 26 et 27 octobre 2023 et visait à renforcer l'expérience, les connaissances et les compétences des entreprises locales et étrangères et des institutions des secteurs public et privé opérant dans le domaine de la cybersécurité, des infrastructures critiques et des secteurs de la finance et des télécommunications.

Lors de la conférence internationale sur la cyberdiplomatie organisée par l'Institut national de recherche et de développement en informatique en avril 2023 en Roumanie, il a été décidé que l'Azerbaïdjan accueillerait la prochaine conférence en 2024.

Grâce aux activités pratiques menées en vue de former et de développer l'écosystème national dans le domaine de la cybersécurité, la position de l'Azerbaïdjan dans les classements internationaux s'est considérablement améliorée. Selon l'indice mondial de cybersécurité 2020 de l'Union internationale des télécommunications, l'Azerbaïdjan a gagné 15 points et arrive à la quarantième place sur 194 pays avec un score de 89,31.

En ce qui concerne la collaboration internationale dans le domaine mentionné, des participants des différentes agences de la République d'Azerbaïdjan ont assisté aux événements internationaux consacrés à la coopération dans la lutte contre les cybermenaces, à l'échange d'informations et d'expériences sur les cyberincidents et à l'élaboration de politiques et de stratégies dans le domaine de la cybersécurité. Il s'agit notamment des réunions 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, des événements organisés dans le cadre de CyberEast (comité intergouvernemental à composition non limitée), de l'Agence de l'Union européenne pour la formation des services répressifs et des projets de formation et de partenariat opérationnel contre la criminalité organisée financés conjointement par l'Union européenne et le Conseil de l'Europe.

Canada

[Original : anglais]
[16 avril 2024]

La tendance à l'augmentation des activités malveillantes dans le cyberespace ces dernières années renforce la nécessité de travailler efficacement à l'atténuation des menaces susceptibles de compromettre la sécurité et la stabilité internationales.

La collaboration accrue et les efforts concrets qui s'imposent doivent aller de pair avec la création d'un mécanisme de l'Organisation des Nations Unies sur la cybersécurité. Le Canada souligne qu'il importe de s'appuyer sur l'acquis collectif (les normes existantes et notre compréhension commune de la manière dont le droit international s'applique) et de créer un espace dans lequel des discussions plus approfondies, concrètes et techniques peuvent avoir lieu, et sont en lien intrinsèque avec les débats en plénière. Le Canada estime que le futur dialogue institutionnel régulier devrait fonctionner comme un cycle vertueux d'évaluation des menaces, de discussions sur l'application du cadre, de renforcement des capacités et d'examen des lacunes recensées et devant être comblées. Travailler sur des questions réelles, ou sur des scénarios qui imitent ces questions, est plus susceptible de mettre en lumière des solutions d'atténuation tangibles. Le futur dialogue institutionnel régulier devrait être orienté vers l'action et les résultats et démontrer des progrès durables et mesurables.

En tant que propriétaires et exploitants de l'infrastructure du cyberespace, les membres de la communauté des parties prenantes sont nos yeux et nos oreilles sur le terrain et sont particulièrement bien placés pour apporter une contribution unique et de grande qualité, de manière consultative, à nos travaux. La garantie d'une participation importante des parties prenantes au futur dialogue institutionnel régulier sera déterminante pour atteindre l'objectif commun de maintien de la cyberstabilité. Dialoguer de cette manière avec la communauté des parties prenantes constitue aussi l'approche la plus prometteuse pour améliorer et faciliter les possibilités d'inclusion des petits États et des États en développement dans nos activités, et permet, ensuite, de maximiser le potentiel d'amélioration de la cyberrésilience mondiale pour toutes et tous. S'il est réellement inclusif, le futur dialogue institutionnel régulier a plus de chances de recevoir l'adhésion qui peut permettre la mise en œuvre et le

développement de bonne foi d'un comportement responsable des États dans le cyberespace.

Les préoccupations et les intérêts de tous les États, y compris en ce qui concerne l'évolution du cadre, devraient être pris en compte dans le futur dialogue institutionnel régulier, par une participation égale des États aux activités de l'Organisation des Nations Unies. Les décisions relatives aux questions de fond devraient être adoptées par consensus.

Le Canada rappelle et réitère les vues qu'il a exprimées sur le futur dialogue institutionnel régulier dans le cadre du rapport du Secrétaire général sur un programme d'action, comme suite à la résolution 77/37 de l'Assemblée générale adoptée en avril 2023. Ces vues montrent notamment que le Canada salue les rapports et recommandations adoptés par consensus à ce jour (par exemple les rapports publiés en 2021 par le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale). Le Canada estime que la meilleure façon pour ce groupe de travail à composition non limitée de s'acquitter de son mandat, tel qu'il est défini dans la résolution 75/240 de l'Assemblée générale, est de décider d'un dialogue institutionnel à voie unique, permanent, orienté vers l'action et ouvert à toutes et à tous.

Le Canada se réjouit de l'occasion qui lui est donnée de donner son avis, une fois de plus, sur le futur dialogue institutionnel régulier. Il considère que le mécanisme actuel du groupe de travail à composition non limitée n'est ni optimal ni suffisant pour atteindre les objectifs collectifs. Il n'est pas favorable à une répétition ou à un renouvellement permanent du mécanisme actuel du groupe de travail à composition non limitée. Au contraire, il est fermement convaincu qu'un programme d'action, élaboré au sein du groupe de travail à composition non limitée et, dans l'idéal, adopté par consensus, est le meilleur moyen d'assurer un dialogue institutionnel unique, permanent, orienté vers l'action et inclusif sur la cybersécurité. Ce processus permettrait un engagement plus ciblé envers l'application des normes et une discussion plus approfondie sur la manière dont le droit international s'applique. Il assurerait également une meilleure coordination, orientée vers l'action (une telle coordination n'existe pas dans le groupe de travail à composition non limitée actuel), entre la discussion sur la mise en œuvre concrète de l'acquis et le renforcement ciblé des capacités.

Le Canada rappelle que des discussions de fond sur le programme d'action en tant que futur dialogue institutionnel régulier ont eu lieu depuis 2021, notamment dans le cadre du document de travail diffusé dans ce groupe de travail à composition non limitée[9]. Il reconnaît et soutient les appels lancés par d'autres États Membres en faveur d'un processus unique visant à discuter de la cybersécurité à l'Organisation des Nations Unies. À ce titre, le Canada met en garde contre la création d'un processus parallèle distinct pour un dialogue institutionnel régulier qui viendrait concurrencer le programme d'action qui a reçu le soutien de 161 États Membres via la résolution 78/16. Il s'agirait d'une duplication injustifiée et inutile, qui imposerait aux États Membres des coûts de personnel et des coûts financiers inutiles.

La structure et le fonctionnement du programme d'action seront décidés lors d'une conférence internationale, au cours de laquelle une déclaration politique sera adoptée. Il est envisagé que le programme d'action soit géré par le Bureau des affaires de désarmement, qui en assurerait le secrétariat. Il y aura des conférences d'examen

[9] Voir https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf (en anglais).

visant à fournir une orientation stratégique, des discussions plénières ouvertes semblables à celles qui existent dans le cadre du mécanisme actuel des groupes de travail à composition non limitée, et des réunions techniques ou des groupes de travail visant à coordonner les éléments des discussions thématiques qui sont pertinents pour faire face à des menaces précises (par exemple, recenser les activités de renforcement des capacités les plus pertinentes pour mettre en œuvre les normes et appliquer le droit international aux logiciels rançonneurs).

Le programme d'action exploitera les investissements réalisés dans le renforcement des capacités et l'assistance technique, qui sont essentiels pour favoriser un comportement responsable des États dans le cyberespace et faciliter la coopération entre les États. Il créera un dialogue régional grâce à la coopération avec les organisations régionales, dans le but de tirer parti des synergies et de coordonner les initiatives.

Dans le cadre du programme d'action, on ne se contentera pas de publier des rapports de la présidence : des progrès durables et mesurables seront obtenus. On s'efforcera de combler le fossé entre l'acquis et la pratique réelle en renforçant les engagements et en participant à des mécanismes de rapport ou d'examen pour permettre des activités optimales de renforcement des capacités afin d'améliorer le comportement responsable des États dans le monde entier.

Chine

Original : chinois
29 avril 2024

Observations du Gouvernement chinois sur un futur mécanisme permanent de dialogue institutionnel.

En ce qui concerne la résolution 78/237 de l'Assemblée générale intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », la position et les vues du Gouvernement chinois sur un futur mécanisme permanent de dialogue institutionnel sont les suivantes :

> La question d'un futur mécanisme permanent revêt une grande importance pour ce qui est des travaux à venir de l'Organisation des Nations Unies sur les questions de sécurité de l'information. La Chine soutient la mise en place d'un futur mécanisme permanent unique aux fins d'un dialogue institutionnel sur la cybersécurité, avec une participation universelle, dans le cadre de l'Organisation. Parvenir à un consensus sur un futur mécanisme permanent dans le cadre du groupe de travail à composition non limitée est le seul choix qui s'offre à l'ensemble des parties. La Chine n'est favorable à aucune tentative d'établir un mécanisme permanent en dehors du groupe de travail. Elle s'oppose à ce que les travaux repartent de zéro, ce qui entraînerait une division dans les processus de sécurité de l'information de l'Organisation et alimenterait la discorde géopolitique et la confrontation entre les blocs. Cette situation ne bénéficie à aucun des États Membres.
>
> En ce qui concerne la structure et les fonctions du futur mécanisme permanent, celui-ci devrait consolider les résultats importants obtenus dans le maintien des processus de sécurité de l'information de l'Organisation des Nations Unies au cours des 26 dernières années et rechercher un développement à long terme pour l'avenir. Cette structure pourrait être composée de deux volets : un angle « rétrospectif », axé sur le respect et la mise en œuvre de l'actuel cadre de comportement responsable des États dans le cyberespace, en particulier aux fins de l'enrichissement et de l'amélioration des plans d'action

pour le renforcement des capacités. Le second volet serait tourné vers l'avenir et s'attacherait à suivre l'évolution de la situation pour formuler de nouvelles normes (notamment en matière de sécurité des données), promouvoir la formulation d'un instrument juridique pertinent et proposer de nouveaux plans d'action pour le renforcement des capacités. La Chine a présenté l'initiative mondiale sur la sécurité des données afin de proposer des solutions pratiques aux problèmes de sécurité des données. L'initiative stipule que les pays ne doivent pas exiger de leurs entreprises qu'elles stockent sur leur territoire des données générées ou obtenues à l'étranger ; ils doivent respecter la souveraineté, la juridiction et le droit des autres pays à gérer la sécurité des données et ne doivent pas accéder directement aux données d'entreprises ou de personnes d'autres pays sans l'autorisation légale de ces pays. Dans le cadre de l'initiative, des propositions précises pour la protection des infrastructures critiques et la sécurité de la chaîne d'approvisionnement ont été présentées. Le texte de l'initiative a été distribué comme document officiel de l'Assemblée générale des Nations Unies. La Chine est prête à travailler avec toutes les parties pour promouvoir l'élaboration de règles internationales de gouvernance numérique qui reflètent les souhaits et respectent les intérêts de toutes les parties.

Le futur mécanisme permanent devrait être dirigé par les États Membres tout en garantissant la participation de plusieurs parties prenantes, comme c'est actuellement le cas au sein du groupe de travail à composition non limitée. Des conférences d'examen pourraient être organisées tous les cinq ans, avec deux ou trois sessions plénières par an. Au cours des trois premières années du cycle d'examen, des discussions de fond ciblées pourraient avoir lieu, des rapports annuels pourraient être adoptés et des décisions sur des questions importantes présentant un intérêt majeur pour les États Membres pourraient être adoptées par consensus. Au cours de la quatrième année du cycle d'examen, le processus préparatoire de la conférence d'examen pourrait être lancé et des textes évolutifs pourraient être rédigés au nom de la présidence. Au cours de la cinquième année du cycle d'examen, des discussions de fond pourraient avoir lieu, principalement sur la base du texte évolutif de la présidence : un consensus de fond pourrait être obtenu ou négocié et les travaux pour les cinq années suivantes pourraient être définis.

La Chine est prête à continuer à participer activement au processus concerné et à contribuer à la mise en place du futur mécanisme permanent.

Elle espère qu'il sera tenu compte des observations qui précèdent dans les rapports du Secrétaire général portant sur le sujet.

Cuba

[Original : espagnol
29 avril 2024]

Le développement des technologies de l'information et des communications a des retombées de plus en plus importantes sur toutes les sphères de la société. Nous devons éviter que ces progrès n'affectent la sécurité des États.

Cuba réaffirme que ces technologies doivent être utilisées de manière pacifique et que les États doivent se comporter de manière responsable, pour le bien commun de l'humanité, afin de promouvoir le développement durable de tous les pays.

Nous réaffirmons que la coopération entre tous les États est le seul moyen d'éviter que le cyberespace ne devienne le théâtre d'opérations militaires.

Il est impératif d'adopter, dans le cadre de l'Assemblée générale des Nations Unies, un instrument international juridiquement contraignant qui complète le droit international applicable, apporte des réponses aux lacunes juridiques en matière de cybersécurité et affronte efficacement les défis et les menaces croissants auxquels nous sommes confrontés.

À cette fin, le meilleur cadre possible est le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

Le rôle de ce groupe inclusif et transparent, dont l'objectif est de nouer un dialogue intergouvernemental régulier dans le domaine de la sécurité et de l'utilisation des technologies de l'information et des communications, devrait être respecté et préservé. Nous préconisons de poursuivre les travaux sous cette forme, ce qui permettra d'obtenir des résultats consensuels pour tous les États.

Tous les États doivent respecter les normes internationales existantes dans ce domaine. L'accès aux systèmes informatiques et systèmes de télécommunications d'un autre État ne peut se faire que dans le respect des accords de coopération internationaux et avec le consentement de l'État concerné. Les modalités et la nature des échanges doivent être conformes à la législation de cet État.

L'utilisation hostile des télécommunications dans le but déclaré ou dissimulé de renverser l'ordre juridique et politique des États constitue une violation des normes internationalement reconnues dans ce domaine et une utilisation illégale et irresponsable de ces moyens de communication.

L'espace radiophonique cubain est régulièrement violé par des personnes ou entités étrangères qui y diffusent des émissions de radio et de télévision illégales, notamment des programmes visant à inciter au renversement de l'ordre constitutionnel établi par le peuple cubain.

En moyenne, en 2023, plus de 7 000 heures d'émissions contre Cuba ont été illégalement diffusées chaque mois sur 21 fréquences différentes, depuis le territoire des États-Unis, en violation des buts et principes de la Charte des Nations Unies, du droit international et des dispositions de l'Union internationale des télécommunications.

Le blocus économique, commercial et financier imposé à Cuba par le Gouvernement des États-Unis depuis plus de 60 ans a de graves incidences sur le peuple cubain, et notamment sur l'utilisation et la jouissance des technologies du numérique.

Nous réaffirmons notre ferme rejet de l'imposition de mesures coercitives unilatérales qui sont contraires au droit international et entravent l'assistance, la coopération et le transfert de technologies.

Dans notre région, le potentiel des technologies de l'information et des communications est reconnu pour apporter de nouvelles solutions aux défis du développement et pour favoriser une croissance économique soutenue, partagée équitable, ainsi que pour réaliser le Programme de développement durable à l'horizon 2030.

Par ailleurs, il faut promouvoir un environnement numérique ouvert, sûr, stable, accessible et pacifique, comme indiqué dans la déclaration du VIII^{e} sommet de la Communauté des États d'Amérique latine et des Caraïbes, qui se tiendra à Kingstown en 2024.

Cuba réaffirme que la coopération internationale est essentielle pour faire face aux dangers associés à l'utilisation abusive des technologies de l'information et des communications.

Danemark

[Original : anglais]
[1er mai 2024]

Le Danemark considère que l'application du cadre de comportement responsable des États en matière d'utilisation du numérique est essentielle pour garantir un cyberespace mondial, ouvert, stable et sécurisé. La communauté internationale reconnaît que le droit international en vigueur et la Charte des Nations Unies dans son intégralité s'appliquent à l'environnement numérique, et le Danemark reste attaché à la mise en œuvre de ce cadre en ce qui concerne le cyberespace.

Ces 20 dernières années, des progrès importants ont été accomplis dans l'élaboration d'un cadre consolidé de comportement responsable des États dans le cyberespace, y compris l'application du droit international, des normes volontaires ainsi que le renforcement des capacités et des mesures de confiance. Le cadre a été approuvé à plusieurs reprises par consensus par l'Assemblée générale, comme tout récemment dans le rapport d'activité annuel de 2023 du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

Le Danemark, comme l'Union européenne, estime que certaines parties de la résolution 78/237 intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », adoptée par l'Assemblée générale le 22 décembre 2023, reposent sur un texte qui n'a pas fait l'objet d'un consensus. Plus précisément, l'alinéa 16 du préambule et le paragraphe 5 se fondent sur des propositions soutenues uniquement par un groupe limité d'États. Le Danemark craint que cela ne conduise à une réinterprétation des documents de consensus existants. Par conséquent, il n'a pas été en mesure d'appuyer la résolution 78/237.

En ce qui concerne la demande formulée au paragraphe 8 de la résolution

L'ONU a appelé à maintes reprises à la mise en place d'un mécanisme permanent des Nations Unies chargé des questions cyber dans le contexte de la sécurité internationale. L'Assemblée générale a répondu à cet appel en octobre 2023 lorsqu'elle a pris la décision d'établir 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.

Des progrès notables ont été accomplis dans les débats sur le futur mécanisme, et le Danemark souhaiterait formuler les observations supplémentaires ci-dessous concernant le dialogue institutionnel régulier à venir.

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 (2019-2021), qui a conclu que le futur dialogue institutionnel devrait être « orienté vers l'action et assorti d'objectifs précis, élargir la portée des réalisations précédentes et être inclusif, transparent, fondé sur le consensus et axé sur les résultats »[10].

Le programme d'action devrait constituer un mécanisme permanent et institutionnel qui permettra de suivre l'application des normes convenues, d'appuyer et de promouvoir le renforcement des capacités, et d'aider à formuler des recommandations et de les actualiser régulièrement. En outre, il devrait être souple

[10] A/75/816, par. 74.

afin que l'on puisse poursuivre l'élaboration du cadre, sur la base des enseignements tirés du respect des engagements existants.

Le Danemark juge qu'il est essentiel de reconnaître que toutes les parties prenantes ont un rôle important à jouer dans la construction de l'avenir de la cybersécurité. Afin de garantir un dialogue inclusif, il est primordial de permettre aux parties prenantes concernées, telles que les entreprises, les organisations non gouvernementales et les milieux universitaires, de participer officiellement aux consultations et d'échanger continuellement leurs vues. Cette démarche témoigne d'une volonté de tirer parti de la sagesse collective issue de diverses perspectives. Son caractère inclusif est essentiel à l'instauration d'un dialogue constructif et global qui permette d'aborder les enjeux multidimensionnels de la cybersécurité.

On pourrait organiser des réunions officielles annuelles dans le cadre du programme d'action et permettre à des réunions techniques et à des groupes de travail axés sur des aspects particuliers de se réunir tout au long de l'année. Dans le cadre du futur mécanisme, on devrait convoquer des conférences d'examen périodiques pour revoir le cadre de comportement responsable des États, le mettre à jour si nécessaire et donner une orientation stratégique aux travaux du mécanisme.

Pendant le reste du cycle du groupe de travail à composition non limitée, il faudrait consacrer du temps et des efforts à l'élaboration de certains aspects du programme d'action. Afin d'assurer une transition sans heurt vers le programme d'action, il convient d'examiner les incidences budgétaires d'un mécanisme permanent et de déterminer les acteurs compétents à l'ONU qui pourront s'acquitter de ces fonctions à l'avenir.

Égypte

[Original : anglais]
[26 février 2024]

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 grâce aux évaluations et recommandations faites par les groupes d'experts gouvernementaux en 2010, 2013, 2015 et 2021, et 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 en 2021[11], ce qui a ainsi permis d'élaborer un cadre cumulatif et évolutif pour promouvoir le comportement responsable des États en matière d'utilisation du numérique.

3. Les États Membres sont invités à s'inspirer, en matière d'utilisation du numérique, des rapports de 2010, 2013, 2015 et 2021 des groupes d'experts gouvernementaux ainsi que du rapport 2021 et des premier et deuxième rapports d'activité annuels de l'actuel groupe de travail à composition non limitée sur la

[11] Voir A/65/201, A/68/98, A/70/174, A/75/816 et A/76/135.

sécurité du numérique et de son utilisation (2021-2025). 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. Une proposition de programme d'action des Nations Unies visant à promouvoir un comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale a été faite par l'Égypte et la France en 2020 et élaborée depuis lors par un groupe interrégional d'États ; le programme d'action est abordé dans les rapports finaux du Groupe d'experts gouvernementaux et dans le rapport publié en 2021 par le groupe de travail à composition non limitée, ainsi que dans les premier et deuxième rapports d'activité annuels de l'actuel groupe de travail à composition non limitée.

6. Le Secrétaire général a publié un rapport (A/78/76) qui recense les vues des États sur la portée, la structure, les principes, la teneur, les travaux préparatoires et les modalités de mise en place du programme d'action.

7. Tout futur mécanisme de dialogue institutionnel régulier doit faire fond sur l'acquis et le cadre convenu existant qui a déjà été approuvé par consensus par l'Assemblée générale.

8. Le nouveau mécanisme ou la nouvelle plateforme sera établi(e) à l'expiration du mandat de l'actuel groupe de travail à composition non limitée, après 2025. Ce dispositif permettrait ainsi d'éviter les doubles emplois ou la tenue d'activités en parallèle. Sous les auspices de l'ONU, il servirait de guichet unique et de plateforme globale pour traiter des questions relatives aux progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et pour promouvoir le comportement responsable des États en matière d'utilisation du numérique.

9. Les États Membres sont convenus en principe que le mécanisme de dialogue institutionnel régulier serait à voie unique, dirigé par les États, permanent, inclusif, transparent et souple[12].

II. Objectifs et portée du futur mécanisme des Nations Unies destiné à favoriser le dialogue institutionnel régulier

10. Servir de plateforme de dialogue institutionnel régulier permettant à tous les États Membres de participer à un mécanisme à voie unique, permanent, inclusif, transparent, orienté vers l'action et fondé sur les résultats et le consensus, et s'appuyant sur le cadre existant.

11. Promouvoir un environnement numérique ouvert, sûr, stable, accessible, pacifique et interopérable.

12. Prévenir les conflits que l'utilisation du numérique peut engendrer et chercher à régler les différends par des moyens pacifiques.

13. Intégrer durablement les outils cyber existants (répertoire d'interlocuteurs et toutes les autres propositions que le groupe de travail à composition non limitée adoptera) en vue de maintenir leur efficacité et de les réexaminer, le cas échéant.

[12] A/78/265, par. 55.

14. Élaborer des orientations concrètes pour aider les États Membres à appliquer les normes, règles et principes convenus, notamment en encourageant la coopération et l'assistance internationales.

15. Sa portée devrait s'articuler autour des trois piliers suivants :

1) **Application des textes arrêtés** : 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 normalisé de rapport qu'il convient de suivre).

2) **Développement du cadre existant** : 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 reprendre les délibérations sur des questions conceptuelles telles que l'applicabilité du droit international ou la nécessité d'élaborer de nouvelles règles et obligations juridiquement contraignantes dans ce domaine.

3) **Promotion du renforcement des capacités** : 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 ; 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) ; 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 précis pour les activités pertinentes, en s'appuyant notamment sur des instruments existants ou nouveaux, comme le fonds d'affectation spéciale multidonateur de la Banque mondiale pour la cybersécurité.

III. Création du futur mécanisme des Nations Unies destiné à favoriser le dialogue institutionnel régulier

16. Les vues et les propositions présentées par les États Membres dans le cadre de l'actuel groupe de travail à composition non limitée sur la proposition de programme d'action et dans les rapports du Secrétaire général présentés en application des résolutions 77/380 et 78/237 de l'Assemblée générale ainsi que les recommandations pertinentes figurant dans les rapports du groupe de travail à composition non limitée devraient servir à définir la portée, la structure et les modalités du mécanisme.

17. Les États Membres devraient continuer à participer activement à l'actuel groupe de travail à composition non limitée, créé en application de la résolution 75/240 de l'Assemblée générale, en vue de produire des rapports de consensus, y compris des recommandations sur la mise en place du futur mécanisme de dialogue institutionnel régulier.

18. Le mécanisme devrait être étoffé et mis au point au sein de l'actuel groupe de travail à composition non limitée 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.

19. Le mécanisme doit être établi après la fin du mandat de l'actuel groupe de travail à composition non limitée, en 2025, en s'appuyant sur les recommandations formulées dans le rapport final de ce groupe de travail, tandis que l'on pourrait envisager la possibilité de créer le futur dialogue institutionnel régulier par une

résolution de consensus de l'Assemblée générale fondée sur des consultations et des préparatifs inclusifs et transparents. Dans le cadre de l'actuel groupe de travail à composition non limitée, les États Membres pourraient convenir d'établir le mécanisme, y compris les modalités proposées, au moyen d'une déclaration politique qui pourrait être entérinée par une résolution de l'Assemblée générale. Le document final issu du Sommet de l'avenir pourrait inclure une référence à un accord initial sur cette question.

IV. Structure et modalités possibles

Réunions périodiques

20. Ce mécanisme, qui pourrait prendre la forme d'un programme d'action, devrait prévoir l'organisation, tous les six ans, d'une conférence d'examen visant à :

a) examiner l'application du mécanisme 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.

21. Le mécanisme devrait tenir des réunions biennales régulières pour mettre en œuvre le programme de travail adopté par la Conférence d'examen et assurer le suivi de l'application des normes, règles et principes convenus par les États Membres en examinant leurs rapports nationaux périodiques d'exécution.

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

23. Dans le cadre du mécanisme convenu, il pourrait 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

24. Dans le cadre du mécanisme convenu, les États Membres seraient encouragés à soumettre 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 des Nations Unies en matière d'utilisation responsable du numérique par les États dans le contexte de la sécurité internationale. Les États Membres pourraient aussi inclure dans leurs rapports nationaux de mise en œuvre une section décrivant leurs priorités et leurs besoins en matière de renforcement des capacités.

25. À l'issue de chaque réunion biennale et de chaque conférence d'examen devrait 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

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

Secrétariat

27. Le Bureau des affaires de désarmement devrait assurer le secrétariat du mécanisme.

Participation des parties prenantes

28. Le mécanisme est un processus intergouvernemental dans lequel la négociation et la prise de décisions sont des prérogatives des États Membres.

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

30. Les organisations non gouvernementales compétentes dotées du statut consultatif auprès du Conseil économique et social en application des dispositions de sa résolution 1996/31 indiqueront au secrétariat qu'ils souhaitent participer aux travaux du programme d'action.

31. Les autres organisations non gouvernementales intéressées dotées d'une expérience et de compétences pertinentes eu égard à la portée et à la finalité du mécanisme informeront également le secrétariat de l'intérêt qu'elles ont 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 mécanisme. Les organisations sélectionnées seront invitées à participer aux sessions officielles du mécanisme, en qualité d'observatrices, selon la procédure d'approbation tacite.

32. 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.

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

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

34. Le mécanisme peut faciliter la coordination avec les initiatives régionales et sous-régionales pertinentes en les invitant notamment à participer et à présenter des contributions.

Estonie

[Original : anglais]
[30 avril 2024]

En application des dispositions de la résolution 78/237 de l'Assemblée générale, l'Estonie souhaite présenter une position nationale sur le futur dialogue institutionnel régulier sur la sécurité du numérique et de son utilisation.

Ces 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 à composition non limitée.

À la suite du large appui apporté par un groupe interrégional de pays à l'élaboration d'un programme d'action, l'Estonie soutient ce dernier en tant que mécanisme institutionnel permanent relevant de la Première Commission, axé sur l'application du cadre de comportement responsable des États dans le cyberespace convenu, tout en permettant de poursuivre le développement de ce cadre, le cas échéant. L'Estonie estime qu'un tel dialogue institutionnel régulier contribuerait à réduire les tensions, à prévenir les conflits et à favoriser l'utilisation pacifique du numérique.

La présente position nationale est une mise à jour de la contribution nationale de l'Estonie figurant dans le rapport du Secrétaire général sur le programme d'action (A/78/76), qui s'appuie, entre autres, sur les progrès reflétés dans la résolution 78/16 de l'Assemblée générale et sur les débats menés dans le cadre du groupe de travail à composition non limitée (2021-2025).

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 convenus et le cadre de comportement responsable des États. Elle insiste 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 des Groupes 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 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 continuer 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 mécanisme d'ici 2026, comme convenu dans la résolution 77/37 de l'Assemblée générale. Elle estime qu'avec le format proposé pour le programme d'action, l'Assemblée 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 à composition non limitée. Les débats menés par l'actuel groupe de travail à composition non limitée ont été constructifs et se sont appuyés 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.

4. **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 leurs compétences spéciales et de leurs connaissances**. La participation de la communauté multipartite aidera les États Membres à appliquer le cadre de comportement responsable des États et à concevoir et mettre en œuvre des initiatives de renforcement des capacités axées sur les besoins afin d'accroître la cyberrésilience à l'échelle mondiale. De même, dans le cadre du programme d'action, on pourrait renforcer l'engagement régional en coopérant avec les organisations régionales et thématiques afin de consolider les initiatives existantes pertinentes et d'en tirer parti.

5. Le **programme d'action devrait prévoir un format plus flexible et axé sur l'essentiel, qui permettrait de poursuivre des débats sur le cadre de comportement responsable des États.** L'Estonie tient à 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.

a) Elle suggère d'inclure parmi les éléments du mécanisme du Programme d'action, des séances plénières annuelles consacrées à des questions relevant des principaux piliers du cadre de comportement responsable des États.

b) Elle est également favorable à des débats ciblés au sujet de la structure des groupes de travail, qui seraient ouverts à toutes les personnes intéressées et porteraient notamment sur les menaces, le renforcement des capacités, la consolidation 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. La participation aux groupes de travail devrait se faire sur une base volontaire et la création de ces derniers serait décidée par les États lors des séances plénières annuelles.

c) Elle soutient également la tenue de conférences d'examen (par exemple, tous les quatre ans) qui permettraient aux participantes et participants de faire le point sur les progrès accomplis et d'envisager d'éventuelles modifications supplémentaires du mandat ainsi que de l'organisation des travaux ou des activités du programme d'action.

6. Le **programme d'action devrait entre autres 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. 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. En particulier, le programme d'action pourrait offrir une plateforme pour l'examen des éléments suivants lors des débats sur le droit

international : a) poursuite des échanges sur l'application du droit international au cyberespace ; b) échange de vues nationales ; c) réunions consacrées à l'application du droit international à l'utilisation du numérique, axées sur des thèmes précis permettant un examen plus approfondi ; d) exposés présentés par des expertes ou des experts ; e) débats fondés sur des scénarios ; f) renforcement des capacités en matière de droit international.

7. Le **programme d'action devrait être orienté vers l'action et largement 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. Le programme d'action pourrait également encourager la communication volontaire de rapports sur les initiatives nationales de mise en œuvre, ce qui contribuerait à la réalisation de nombreux objectifs tels que le renforcement de la confiance, la transparence et l'évaluation des capacités et des besoins. 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 de l'Union européenne, qui recense les projets de renforcement des cybercapacités des États membres de l'Union européenne.

États-Unis d'Amérique

[Original : anglais
1er mai 2024]

Introduction

Les États Membres de l'Organisation des Nations Unies ont constaté 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 chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), 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 au départ en 2015 dans le rapport de consensus du Groupe d'experts gouvernementaux, les États ont affirmé qu'il était nécessaire d'instaurer un dialogue institutionnel régulier à large participation sous les auspices de l'ONU[13]. S'appuyant sur cet effort, le groupe de travail à composition non limité n'a cessé de réaffirmer, depuis, que les États devaient s'efforcer de créer un mécanisme favorisant le dialogue institutionnel[14].

En outre, comme indiqué dans le dernier rapport annuel consensuel du groupe de travail à composition non limitée, les États se sont mis d'accord sur une première

[13] A/70/174, par. 18.
[14] A/75/816, par. 70 à 74, et A/78/265, par. 52.

série d'éléments communs du dialogue institutionnel régulier et ont aussi décidé de poursuivre les discussions sur un futur programme d'action. Il importe de noter qu'ils sont convenus que le futur dialogue institutionnel régulier « s'appuierait sur les accords consensuels obtenus sur le cadre de comportement responsable des États »[15]. Ils ont aussi décidé que le dialogue futur devrait être unique, dirigé par les États et permanent[16]. Ils ont également conclu que le mécanisme devrait être ouvert, inclusif, transparent, durable et flexible[17] afin qu'il puisse s'adapter si nécessaire à l'évolution rapide des cybermenaces. Dans son rapport publié en avril 2023 (A/78/76), le Secrétaire général a souligné qu'il était urgent de créer le programme et mis en évidence un grand nombre de questions traitées par les éléments communs mis au jour dans le rapport d'activité annuel du groupe de travail à composition non limitée en 2023, notamment le fait que le cadre « devait servir de point de départ » pour le programme d'action[18]. Dans son rapport, le Secrétaire général a conclu que de nombreux États appréciaient la participation inclusive et utile des parties prenantes non gouvernementales[19]. Les États ont continué de demander la pleine participation de toutes les parties prenantes aux réunions formelles et intersessions du groupe de travail à composition non limitée.

Au cours des deux dernières années, les États se sont ralliés au programme d'action en tant que futur mécanisme permanent pour les discussions de la Première Commission de l'Organisation des Nations unies sur les questions cyber. Plus récemment, la quasi-totalité des États Membres ont voté en faveur de la résolution 78/16, par laquelle l'Assemblée générale a établi de manière décisive le mécanisme sous les auspices de l'Organisation des Nations Unies, à l'issue des travaux de l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation.

Comme le souligne la résolution, le programme d'action servira de mécanisme à la fois permanent et flexible qui fera progresser le cadre afin d'améliorer la paix et la sécurité dans le cyberespace, notamment par un dialogue important avec la communauté multipartite et par la facilitation du renforcement des capacités grâce au rôle de l'Organisation en tant que plateforme d'échange d'informations.

Portée du programme d'action

La résolution 77/37 de l'Assemblée générale a défini la portée et le mandat du programme d'action comme suit :

Un mécanisme permanent, inclusif et orienté vers l'action qui permettra d'examiner les menaces existantes et potentielles ; de renforcer les capacités des États et d'appuyer les efforts faits par les États pour mettre en œuvre et promouvoir les engagements pris au titre du cadre de comportement responsable, 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, comme le prévoient sa résolution 76/19, les rapports de 2010, 2013, 2015 et 2021 des groupes d'experts gouvernementaux, le 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 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) ; d'étudier ce cadre et de le développer, le cas échéant ; de promouvoir le

[15] A/78/265, par. 55 c).
[16] Ibid., par. 55 a).
[17] Ibid., par. 55 d).
[18] A/78/76, par. 42.
[19] A/78/76, par. 40.

dialogue et la coopération avec les parties concernées, et d'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[20].

Dans sa résolution 78/16, l'Assemblée générale a réaffirmé les objectifs du programme d'action tels qu'énoncés dans la résolution 77/37 et décidé que le mécanisme comporterait les éléments communs décrits dans le rapport d'activité du groupe de travail à composition non limitée pour 2023. Elle a aussi décidé que la portée, la structure, le contenu et les modalités du programme d'action seraient basés sur les résultats consensuels du groupe de travail à composition non limitée.

Dans le cadre des résolutions sur le programme d'action et des résolutions de consensus qui ont confirmé les rapports du groupe d'experts gouvernementaux et du groupe de travail à composition non limitée, les États ont affirmé à plusieurs reprises que les États devraient être guidés dans leurs activités par les constatations et recommandations formulées dans les rapports de 2010, 2013, 2015 et 2021 des groupes d'experts gouvernementaux et le 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, ainsi que par les produits de consensus de l'actuel groupe de travail à composition non limitée (par exemple les premier et deuxième rapports d'activité annuels), et en particulier « le cadre cumulatif et évolutif élaboré dans ce contexte pour promouvoir le comportement responsable des États en matière d'utilisation du numérique et adopté par consensus »[21]. Ce cadre consensuel, défini par les rapports de consensus du Groupe d'experts gouvernementaux et les rapports des groupes de travail à composition non limitée et approuvé à plusieurs reprises par tous les États Membres, constitue le socle du programme d'action.

Les États Membres définiront l'orientation du programme d'action et l'actualiseront au fil du temps, en mettant l'accent en priorité sur l'application pratique et les activités de renforcement des capacités consacrées à la mise en œuvre du cadre. Du fait de sa nature permanente, le programme d'action constituera une ressource durable pour les États dans ces activités.

En tant que mécanisme permanent, le programme d'action doit aussi avoir la souplesse nécessaire pour faire face aux menaces futures et pour évaluer l'évolution des besoins des États et les meilleures pratiques permettant de faire face à ces menaces. Dans le cadre du programme d'action, les États pourront également déterminer si et comment le cadre consensuel doit évoluer au fil du temps.

Les parties prenantes non étatiques feront partie intégrante du dispositif. Presque tous les efforts de renforcement des capacités, qu'ils soient internationaux ou nationaux, font appel aux activités et à l'expertise du secteur privé, de la société civile, du milieu universitaire et d'autres parties prenantes non étatiques. Le programme d'action doit prévoir des modalités de participation aussi inclusives que possible pour bénéficier des compétences de ces acteurs.

Mise en place d'un programme d'action

Les États Membres doivent viser une transition en douceur vers le programme d'action en 2025, après la conclusion des travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Cette transition doit être facilitée par un rapport final du groupe de travail à composition non limitée réaffirmant le mandat du programme tel que défini par la résolution 77/37 de l'Assemblée générale (avec le cadre consensuel comme socle), articulant sa

[20] Résolution 77/37 de l'Assemblée générale, par. 26.
[21] Résolution 78/16 de l'Assemblée générale, par. 8 du préambule.

structure pragmatique et ses méthodes de travail, définissant les domaines de travail prioritaires, confirmant une approche aussi inclusive que possible de la participation des parties prenantes et déterminant les prochaines étapes et le calendrier détaillé du lancement officiel du programme d'ici à 2026.

Pour définir pleinement les modalités du programme d'action, une réunion ou un processus préparatoire supplémentaire peut s'avérer nécessaire. De plus, si le groupe de travail à composition non limitée ne parvient pas à un consensus sur un rapport final, une « conférence internationale »[22] plus complète ou un autre processus préparatoire établi par l'intermédiaire de l'Assemblée générale sera nécessaire pour respecter la résolution 78/16, qui prévoit le lancement du programme d'ici à 2026. Les réunions du programme doivent commencer en 2026 pour assurer la continuité de ces importantes discussions multilatérales.

Étant donné que le programme d'action a pour mandat d'aborder les dimensions de paix et de sécurité de l'utilisation des technologies de l'information et des communications, il sera naturellement établi sous l'égide de la Première Commission. Le Bureau des affaires de désarmement est un secrétariat logique pour ce futur mécanisme. Le programme d'action devrait être exécuté dans la limite des ressources budgétaires existantes, autant que faire se peut.

Structure

La structure du programme d'action devrait comprendre des groupes de travail techniques qui se réunissent trois ou quatre fois par an, des réunions plénières annuelles et des conférences d'examen périodiques. Le programme serait soutenu par un secrétariat au Bureau des affaires de désarmement.

Les groupes de travail techniques du programme d'action constituent l'essence même de sa nature pragmatique, et non un élément facultatif. Pour que ces groupes soient aussi inclusifs que possible, tous les États intéressés seraient invités à travailler ensemble dans des groupes ciblés afin d'élaborer des recommandations concrètes soutenant l'application du cadre. Ces recommandations figureront dans les rapports soumis à l'examen de la plénière et, en dernier ressort, de l'Assemblée générale.

Ces groupes de travail doivent avoir une composition interrégionale et adopter une approche transversale de l'application du cadre, en élaborant des recommandations, des évaluations et des meilleures pratiques sur des questions telles que :

- la défense des infrastructures critiques ;
- la facilitation de la coopération entre les États à la suite d'un cyberincident grave ;
- les moyens d'améliorer l'obligation de rendre compte du comportement irresponsable des États dans le cyberespace ;
- le partage d'informations sur l'évolution des cybermenaces ;
- l'amélioration de la capacité des États de dissuader et mettre en échec les menaces liées au numérique.

Des discussions thématiques faciliteraient un débat de fond transversal sur la mise en œuvre du cadre, qui sortirait des cloisonnements traditionnels entre les menaces, les normes, le droit international et le renforcement des capacités. Dans le groupe de travail à composition non limitée, les États ont souligné à plusieurs reprises que ces questions se recoupaient et qu'elles devaient être examinées de manière globale. Les États conviennent également que le renforcement des capacités, en

[22] Résolution 77/37 de l'Assemblée générale, par. 3.

particulier, est transversal à tous les thèmes. En donnant la priorité à la discussion sur les besoins en matière de renforcement des capacités dans les groupes de travail chargés de l'application, on obtiendra des recommandations réalistes et réalisables et on accélérera ladite application.

La réunion plénière annuelle devrait avoir pour mandat d'évaluer les progrès des groupes de travail techniques, de faire avancer les recommandations de ces groupes, de discuter des menaces actuelles et émergentes et d'examiner l'état d'avancement des initiatives pratiques telles que les mesures de confiance. La plénière peut fournir des orientations aux groupes de travail techniques et aux initiatives pratiques, le cas échéant.

La conférence d'examen périodique devrait se réunir tous les trois ou quatre ans (en remplacement de la réunion plénière annuelle pendant les années de la conférence) pour que tous les États Membres puissent évaluer l'évolution des cybermenaces et les résultats des initiatives et des groupes de travail du programme d'action, mettre à jour le cadre si nécessaire et donner une orientation stratégique et des mandats pour les futures plénières, les groupes de travail et les autres initiatives du programme. Ce réexamen périodique du programme donnerait aux États la possibilité de l'adapter en fonction de l'évolution de la situation.

Chaque année, après le lancement du programme d'action en 2026, la Première Commission confirmera les résultats consensuels des réunions annuelles du programme par une résolution ou une décision. Elle confirmera aussi les résultats des conférences d'examen périodiques lorsqu'elles ont lieu.

Le secrétariat du programme d'action, géré par le Bureau des affaires de désarmement, serait chargé de soutenir la gestion des différentes réunions du programme, de maintenir des plateformes d'échange d'informations, des mécanismes de communication et des archives, et de gérer des initiatives et des projets concrets tels que le répertoire d'interlocuteurs, le répertoire des menaces et les portails d'échange d'informations.

Renforcement des capacités

Étant donné que les pays se trouvent à différentes étapes du développement de leur expertise et de leurs compétences dans le domaine des technologies de l'information et des communications, l'Organisation des Nations Unies a reconnu que « le renforcement des capacités est indispensable à la coopération entre les États et au renforcement de la confiance dans le domaine de la sécurité numérique »[23]. L'Organisation a un rôle clef à jouer pour ce qui est de rassembler, de coordonner et de mettre en avant les multiples parties prenantes qui travaillent activement au renforcement des capacités liés à différentes questions cyber et au déploiement des programmes sur la base des orientations données par les États Membres.

La fonction première de renforcement des capacités du programme d'action doit être directement liée aux efforts déployés par les États au niveau national pour mettre en œuvre le cadre. Le programme d'action devrait aussi faciliter les discussions portant sur les types de renforcement des capacités dont les États ont besoin pour appliquer le cadre, afin que ses activités soient étroitement alignées sur ces besoins. En d'autres termes, il devrait viser à sensibiliser la communauté internationale à l'importance du renforcement des cybercapacités afin de soutenir le cadre et de faciliter la coordination et le partage d'informations sur les programmes de renforcement des cybercapacités disponibles avec d'autres parties prenantes, tout en

[23] Ibid., alinéa 20 du préambule.

communiquant des orientations et des meilleures pratiques que les États pourraient utiliser au niveau national pour appliquer le cadre.

Les États-Unis constatent que nombre d'États ne sont pas encore suffisamment informés de la nature et de l'importance du cadre. Beaucoup manquent aussi des capacités nationales de base en matière de cybersécurité, notamment des autorités et capacités nationales associées au soutien des normes et des 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, ou encore la coordination des donateurs et la mise en relation à des fins d'assistance internationale. Le programme d'action ne doit pas faire double emploi ou se substituer à ces efforts existants. Tous ces programmes (qui sont en grande partie multipartites) renforcent la position des États en matière de sécurité nationale et permettent en fin de compte l'application du cadre, bien qu'ils 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, les organismes régionaux et internationaux 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. Les parties prenantes opérant dans ce domaine devraient donc pouvoir participer activement au programme d'action et y contribuer en tant qu'observatrices, sans droit de vote. L'expertise des parties prenantes non gouvernementales sera particulièrement importante dans les groupes techniques ou les groupes de travail. Ces groupes de travail techniques faciliteront un dialogue plus approfondi et concret avec une série de parties prenantes non étatiques. Les parties prenantes pourraient aussi communiquer des rapports périodiques sur leurs efforts visant à mettre en œuvre des initiatives axées sur le cadre, telles que le renforcement des capacités.

Pour que le programme d'action intègre autant que possible les parties prenantes intéressées, y compris dans ses groupes de travail techniques subsidiaires, les modalités devraient s'appuyer sur les normes de référence existantes en matière de participation des parties prenantes, notamment en assurant la transparence quant aux objections des États et en prévoyant un processus d'évaluation des exclusions éventuelles. On pourrait par exemple s'inspirer du règlement du Groupe de travail à composition non limitée sur le vieillissement. Les modalités prévues pour ce groupe permettent aux États Membres de s'opposer à la participation d'une organisation, mais exigent que ces objections soient formulées publiquement pour que les États Membres en soient informés et qu'un vote ultérieur détermine si les organisations pour lesquelles une objection a été formulée doivent être exclues. Les organisations dont la participation n'a soulevé aucune objection au premier tour d'examen sont autorisées à participer à la session officielle[24].

Outre les considérations relatives à la manière dont les parties prenantes sont accréditées pour assister aux réunions tenues au titre du programme d'action, les modalités devraient également donner des orientations sur la manière dont les parties prenantes accréditées peuvent contribuer aux discussions du programme. Dans ce domaine, le Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des

[24] Comme indiqué dans la section F du document A/AC.278/2011/2.

communications à des fins criminelles pourrait servir de modèle. Conformément à son règlement, les diverses parties prenantes peuvent notamment :

- Assister à toute session officielle ouverte.
- 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 disponible pendant les réunions étant limité, elles peuvent designer 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 spécial[25].

Le programme d'action devrait aussi tirer parti de l'expertise existante et des travaux en cours au niveau régional. En permettant à ces entités de participer aux discussions portant sur le programme d'action en tant que parties prenantes, on favoriserait, dans les travaux menés au niveau de l'Organisation, une meilleure prise en compte des efforts, des difficultés et des problématiques propres aux régions.

Fédération de Russie

[Original : russe
9 avril 2024]

Document de réflexion sur l'établissement d'un groupe de travail permanent à composition non limitée doté d'une fonction décisionnelle en matière de sécurité du numérique et de son utilisation

Coauteurs : République du Bélarus, Burkina Faso, République du Burundi, République de Cuba, État d'Érythrée, Fédération de Russie, République du Mali, République de l'Union du Myanmar, République du Nicaragua, République arabe syrienne, République populaire démocratique de Corée, République du Soudan, Venezuela (République bolivarienne du) et République du Zimbabwe

Les discussions menées dans le cadre du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) ont permis de mettre en évidence que la communauté internationale souhaitait la mise en place, sous les auspices de l'Organisation des Nations Unies, d'un mécanisme décisionnel unique et permanent sur cette question. Nous pensons que le format optimal d'un tel mécanisme est un groupe de travail à composition non limitée, lequel a prouvé son efficacité et son utilité dans la pratique.

Le mandat de tout futur groupe de travail permanent à composition non limitée doté d'une fonction décisionnelle devrait être axé sur le renforcement de l'action en faveur d'un environnement numérique ouvert, sûr, stable, accessible et pacifique par l'application concrète des accords conclus dans le cadre du groupe de travail à composition non limitée (2021-2025). Les questions relevant du mandat sont notamment les suivantes :

– La poursuite de l'élaboration de règles, normes et principes juridiquement contraignants sur le comportement responsable des États et la mise en place de mécanismes efficaces en vue de leur application, en tant qu'éléments d'un futur traité universel visant à garantir la sécurité de l'information au niveau international ;

[25] A/AC.291/6, par. 3.

– L'élaboration d'une position commune sur l'application du droit international s'agissant de l'utilisation des outils numériques et sur les possibilités d'adaptation des normes existantes aux spécificités de l'espace informatique (dimension transfrontalière, anonymat et possibilité d'introduire des fonctions cachées) ;

– L'élaboration et l'application de mesures de confiance et de mécanismes de coopération pratique entre les États, notamment au moyen de canaux de coopération établis entre les structures et organismes autorisés et d'un répertoire intergouvernemental mondial d'interlocuteurs, afin de contrer les menaces informatiques pesant sur la sécurité du numérique et de son utilisation et de prévenir les conflits entre États dans l'espace informatique mondial ;

– La mise en place de mécanismes et de programmes destinés à aider les États à améliorer leurs capacités de protection de leurs ressources informatiques nationales, en tenant compte des besoins de chacun.

Les activités du futur groupe de travail permanent à composition non limitée devraient reposer sur les principes suivants :

– L'ouverture, l'inclusion, la démocratie et la transparence ;

– Le rôle de premier plan joué par les États à l'appui du dialogue sur la sécurité de l'utilisation du numérique par les États, sous l'égide de la Première Commission de l'Assemblée générale des Nations Unies ;

– Le respect des principes de la Charte des Nations Unies (égalité souveraine des États, non-recours à la menace ou à l'emploi de la force et règlement pacifique des différends internationaux) ;

– Les décisions doivent être prises par consensus et uniquement par les États ;

– L'inopportunité de reproduire dans différentes instances des Nations Unies le travail mené par la communauté internationale en faveur de la sécurité du numérique et de son utilisation ;

– La prise en compte dans un esprit de continuité des conclusions adoptées par consensus et des recommandations des précédents groupes de travail à composition non limitée et des groupes d'experts gouvernementaux ;

– La flexibilité et la capacité d'évoluer en fonction des besoins des États et des nouveaux enjeux en matière de sécurité du numérique.

Questions de procédure :

– Toute décision prise au sein du groupe de travail permanent à composition non limitée est approuvée par consensus entre les États (ce paramètre doit être clairement énoncé dans la résolution de l'Assemblée générale établissant le groupe de travail permanent à composition non limitée) ;

– Calendrier : le groupe de travail permanent à composition non limitée commence ses travaux quand l'actuel groupe de travail à composition non limitée conclut les siens et tient deux sessions formelles par an au Siège de l'ONU à New York (tous les États Membres, sans exception, doivent être représentés) ;

– Communication de l'information : des rapports d'activité sont présentés à l'Assemblée générale et adoptés par consensus tous les deux ans ;

– Structure : si nécessaire, les États Membres peuvent décider de créer des sous-groupes subsidiaires pour examiner plus en détail et en profondeur des aspects précis du mandat du mécanisme ; toutefois, les réunions de ces sous-groupes ne

doivent pas se tenir simultanément, afin d'assurer la pleine participation de toutes les délégations ;

– Gouvernance : les travaux du groupe de travail permanent à composition non limitée sont menés par un bureau composé d'un(e) président(e), de deux vice-président(e)s, d'un(e) rapporteur(euse) et, le cas échéant, de président(e)s de sous-groupes (assumant également la fonction de vice-président) ; la composition du bureau est approuvée par consensus tous les deux ans par les États et respecte le principe de la répartition géographique équitable, par roulement des groupes régionaux.

Il serait souhaitable de doter le groupe de travail permanent à composition non limitée d'un mécanisme permettant d'officialiser rapidement les décisions à mesure qu'elles sont adoptées (selon la procédure d'approbation tacite donnant lieu à l'adoption lors de la session suivante) et de prendre des mesures pratiques pour assurer un échange continu d'informations entre les États au moyen d'un portail électronique de circonstance.

Il serait utile de prévoir que le groupe de travail permanent à composition non limitée coopère avec les organisations et associations régionales concernées, sous la forme de consultations menées par sa présidence avec des groupes de pays et de réunions intersessions annuelles avec leurs représentants.

La participation des acteurs non étatiques (organisations non gouvernementales, milieux d'affaires et monde scientifique et universitaire) aux travaux du groupe de travail permanent à composition non limitée devrait être de nature purement consultative et informelle, par exemple, une fois par an sous la forme de réunions intersessions. Le droit d'assister à des manifestations officielles en tant qu'observateurs n'est accordé qu'aux acteurs non étatiques qui sont accrédités (par consensus entre les États).

France

[Original : français]
[30 avril 2024]

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 résolutions[26].

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

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

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, [s'appuyer sur les] 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 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 échéant[29]. 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 proposition portée depuis 2020 par un groupe transrégional d'États de mettre en place 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.

Dans son rapport relatif au 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/78/76), le Secrétaire général a 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 (2021-2025), en s'appuyant sur les points de vue exprimés dans le 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.

La présente contribution est une mise à jour de la contribution nationale de la France incluse dans le document A/78/76 qui reflète les avancées permises par la résolution 78/16 de l'Assemblée générale et la poursuite des discussions au sein du groupe de travail à composition non limitée (2021-2025).

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.

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'un dialogue inclusif entre États et avec les parties concernées ;
- la stabilité : promouvoir la stabilité dans le cyberespace 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

[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.

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 pertinents[30]. 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 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 consensus[31] ;

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 plénières, par exemple sur une base annuelle ou semestrielle (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) discuter des menaces existantes et émergentes ; b) envisager la mise en œuvre des normes, règles et principes ; c) 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 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.

---

[30] Notamment la résolution 76/19 de l'Assemblée générale, les rapports de consensus des groupes d'experts gouvernementaux 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 de travail actuel enrichiront ce cadre cumulatif et évolutif.

[31] Voir la résolution 77/37 de l'Assemblée générale, deuxième alinéa, et la résolution 78/16 de l'Assemblée générale, deuxième alinéa.

- Organisation de réunions intersessions afin d'avancer dans le programme de travail convenu lors des réunions annuelles. Ces réunions pourraient être structurées en réunions ou groupes de travail techniques à composition non limitée 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 réunions ou groupes de travail techniques à composition non limitée 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, apporter une expertise technique, discuter des meilleures pratiques et des difficultés, la réunion annuelle pourrait alors décider de créer un axe de travail spécifique, dont les travaux seraient ouverts à tous États et auraient lieu lors des réunions intersessions du programme d'action. Les conclusions et les recommandations de ces réunions ou groupes de travail techniques à composition non limitée seraient remises à la réunion plénière 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

armements[32]. Les initiatives ou les projets financés par cet instrument devraient correspondre à un mandat, qui pourrait être défini par 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 favorisant la tenue de débats sur l'évolution du cadre, notamment en approfondissant la compréhension commune des normes et de la manière dont le droit international existant s'applique à l'utilisation du numérique, en recensant les éventuelles lacunes en la matière et, le cas échéant, en examinant la nécessité de disposer de normes volontaires et non contraignantes supplémentaires ou d'obligations juridiquement contraignantes supplémentaires[33]), 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[34] » 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 demeureraient 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 Commission[35]. La coopération avec ces acteurs peut se révéler essentielle pour

---

[32] Mécanisme de financement des Nations Unies pour la coopération en matière de réglementation des armements, voir https://www.un.org/disarmament/fr/unscar/.

[33] Voir résolution 78/16 de l'Assemblée générale, alinéa 3.b).

[34] A/75/816, annexe I, par. 10.

[35] A/75/816, annexe I, par. 22.

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[36] ». Les acteurs privés peuvent également apporter un savoir-faire précieux aux échanges et contribuer aux efforts de renforcement des capacités.

- 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 discrimination[37]. 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 cyberespace 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.

Les consultations régionales conduites en 2023 et le rapport du Secrétaire général (A/78/76) ont permis de recueillir les points de vue d'un groupe nombreux et diversifié d'États. Le rapport du Secrétaire général souligne que 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. Le deuxième rapport d'activité annuel du groupe de travail à composition non limitée (2021-2025) a permis de poursuivre cette entreprise, en convenant en principe d'« éléments

[36] A/75/816, annexe I, par. 10.

[37] 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).

communs [38] » faisant consensus pour aboutir, de manière constructive, à une conception commune du futur mécanisme de dialogue institutionnel régulier.

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. Dans sa résolution 78/16, l'Assemblée générale insiste 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 à l'issue des travaux du groupe de travail à composition non limitée (2021-2025) et au plus tard en 2026.

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 en 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 futur mécanisme sera mis en place.

Dans sa résolution 77/37, 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 et de petit calibre sous tous ses aspects). Dans sa résolution 78/16, l'Assemblée générale a décidé la création d'un mécanisme placé sous l'égide de l'Organisation des Nations Unies, lequel sera permanent, inclusif et orienté vers l'action et aura pour objectifs ceux énoncés dans la résolution 77/37 et les éléments communs pour un futur dialogue institutionnel régulier établis par consensus dans le deuxième rapport d'activité annuel du groupe de travail à composition non limitée (2021-2025), à l'issue des travaux du groupe de travail à composition non limitée (2021-2025) et au plus tard en 2026. Si les États en décident ainsi, une conférence internationale pourrait être organisée en 2025 afin d'adopter le texte fondateur du dit mécanisme, sur la base des travaux préparatoires accomplis dans le cadre du groupe de travail à composition non limitée (2021-2025).

Cette conférence internationale devrait 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 par 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 mécanisme nouvellement créé.

[38] A/78/265, par. 55.

Géorgie

[Original : anglais]
[20 mars 2024]

En ce qui concerne le futur dialogue institutionnel régulier sur l'utilisation du numérique, instauré sous l'égide de l'Organisation des Nations Unies, la Géorgie considère que 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 constitue le meilleur moyen de promouvoir les initiatives de l'Organisation en matière de cybersécurité et de comportement responsable des États dans le cyberespace.

Dans les conditions de sécurité actuelles, caractérisées par des évolutions géopolitiques rapides et imprévisibles, certains acteurs menacent l'ordre international fondé sur des règles en recourant à la fois à des méthodes de guerre classiques et non classiques. En effet, il arrive malheureusement que des acteurs enfreignent le droit international dans le cadre de cyberopérations. La communauté internationale doit continuer à tenir ces acteurs responsables de leur comportement illicite et inacceptable dans le cyberespace, en veillant à ce que des conséquences juridiques s'ensuivent.

Le programme d'action pourrait servir de plateforme propice à la tenue de dialogues ciblés sur l'application du droit international dans le cyberespace après l'achèvement des travaux, en 2025, de l'actuel groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

La Géorgie recommande que le programme d'action serve de cadre de travail unifié à la Première Commission, axé sur les questions de cybersécurité, de sorte à offrir une structure fiable et propice à la mise en œuvre d'initiatives orientées vers l'action et à l'obtention de progrès tangibles.

L'absence de moyens à l'échelle nationale, régionale et mondiale constitue un défi de taille. Le programme d'action devrait donc aider les pays à mettre en œuvre le cadre normatif et offrir une aide au renforcement des capacités afin de réduire la fracture numérique.

La Géorgie se félicite de la création d'un répertoire mondial et intergouvernemental d'interlocuteurs. Cette initiative marque une étape importante dans le renforcement de la coopération et de la coordination internationales en matière de cybersécurité dans le contexte de l'Organisation des Nations Unies.

Compte tenu du rythme rapide de l'évolution des technologies de l'information et des communications, le futur cadre international doit offrir davantage de flexibilité afin de garantir son utilité future. Cette instance internationale devrait prévoir un mécanisme d'examen périodique du cadre par consensus, facilité par des réunions plénières régulières ou des conférences d'examen, dans le cadre desquelles on pourrait réexaminer le cadre existant et, le cas échéant, décider de l'améliorer ou de le développer davantage.

La Géorgie appuie résolument l'adoption d'une approche multipartite transparente et inclusive et insiste sur la participation active des acteurs étatiques et non étatiques au dialogue institutionnel portant sur ces questions.

Irlande

[Original : anglais]
[1er mai 2024]

En tant que société ouverte dont l'économie est fortement interconnectée et numérisée, l'Irlande est parfaitement consciente de la détérioration des conditions de sécurité à l'échelle internationale, notamment en ce qui concerne l'augmentation des cyberactivités malveillantes. Face à ce problème, elle a pris des mesures au niveau national, ainsi qu'avec ses partenaires de l'Union européenne, pour accroître la résilience, renforcer sa capacité de repérer, prévenir et dissuader les menaces, et promouvoir un cyberespace mondial, ouvert et sûr, fondé sur le droit international et les droits humains.

La position de l'Irlande reste néanmoins sans équivoque, à savoir que la dimension mondiale de ce problème appelle une action internationale globale. L'Irlande a appuyé et jugé encourageant le cadre normatif des Nations Unies élaboré par consensus pour promouvoir un comportement responsable des États en matière d'utilisation du numérique. Il s'agit d'un cadre essentiel, fruit des multiples recommandations par consensus formulées par les groupes d'experts gouvernementaux (2010, 2013, 2015 et 2021) et le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (2021). Le cadre a également été approuvé par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) dans ses deux récents rapports d'activité annuels, adoptés par consensus.

L'année dernière, l'Irlande a affirmé sa position en faveur de l'application du droit international dans le cyberespace, l'un des quatre piliers du cadre normatif. Elle s'est engagée à collaborer avec les autres États membres de l'Union européenne et des partenaires internationaux pour agir conformément au cadre normatif et promouvoir la paix et la stabilité en l'appliquant au niveau mondial.

L'Irlande estime que l'application et le renforcement du cadre normatif sont essentiels au maintien de la sécurité internationale dans le cyberespace et que ces questions devraient donc être au cœur de tout mécanisme de dialogue institutionnel régulier. Le futur cadre de dialogue institutionnel régulier qui pourrait succéder à l'actuel groupe de travail à composition non limitée, tel qu'il est envisagé précisément dans le programme d'action proposé, mesure l'importance que revêt le cadre normatif et prévoit la tenue de conférences d'examen périodiques afin de l'examiner.

L'Irlande a toujours appuyé sans réserve la conception du dialogue institutionnel régulier sur la sécurité du numérique préconisée par le programme d'action, qui prévoit la mise en place d'un mécanisme inclusif et orienté vers l'action en vue d'un futur dialogue permanent. Dans le cadre du programme d'action, il est prévu de mettre en place un dialogue régional inclusif, permanent, multipartite et transparent, qui serait organisé sous les auspices de l'Organisation des Nations Unies. Le programme d'action, tel qu'il est défini dans les résolutions de la Première Commission de l'Assemblée générale, a bénéficié d'un large soutien, comme en témoignent les débats du groupe de travail à composition non limitée et les votes d'un groupe d'États très diversifié sur le plan régional à l'Assemblée.

L'un des éléments essentiels du cadre normatif, à savoir veiller à ce que tous les États puissent tirer parti des avantages offerts par le numérique et atténuer les risques à l'aide de mesures de renforcement des capacités, constitue une priorité pour l'Irlande. Il incombe aux États de réduire la fracture numérique et de renforcer la résilience face aux cyberactivités malveillantes.

La résolution 78/237 de la Première Commission, intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », ne rend pas compte de l'importance du cadre normatif, ni du large éventail de points de vue exprimés par de nombreux États Membres. De ce fait, l'Irlande ne s'est pas trouvée en mesure d'appuyer la résolution et ne pense pas que l'approche qui y est proposée puisse répondre aux besoins de la majorité des États Membres. Au contraire, la résolution pourrait servir à saper la méthode progressive et consensuelle sur laquelle le groupe de travail à composition non limitée s'est appuyé pour réaliser des progrès au cours des dernières années.

Continuant d'espérer qu'un mécanisme de dialogue institutionnel régulier sera établi par consensus avant la fin du mandat de l'actuel groupe de travail à composition non limitée, l'Irlande collaborera avec tous les États pour promouvoir un modèle inclusif et orienté vers l'action qui tienne compte du cadre normatif.

Dans le cadre des débats sur la manière dont l'approche du programme d'action en particulier pourrait s'articuler, on a notamment proposé l'organisation de sessions formelles annuelles, au cours desquelles se tiendraient des débats ouverts et approfondis et des réunions techniques consacrées à des questions stratégiques particulières tout au long de l'année. Les groupes techniques pourraient se pencher sur des questions telles que celles relatives au genre, à la fracture numérique et au rôle des entités non gouvernementales dans la mise en œuvre du cadre normatif. Les axes de travail techniques devraient faire l'objet d'une participation volontaire, être ouverts à tous les États et donner lieu à des conclusions opérationnelles fondées sur les enseignements tirés de l'application du cadre normatif.

Dans le prolongement de l'appui transrégional apporté aux résolutions de la Première Commission, dans lesquelles il est préconisé d'adopter une approche fondée sur un programme d'action, ce mécanisme pourrait aider à accroître la mobilisation à l'échelle régionale et la coopération avec les organisations régionales et à renforcer les capacités en fonction des besoins.

Il est encourageant de constater que le programme d'action, tel que proposé, prévoit également la participation formelle des parties prenantes concernées et la tenue de consultations régulières avec elles, y compris le secteur privé, le milieu universitaire et la société civile, afin qu'elles puissent donner leur avis sur les questions pertinentes. Particulièrement favorable à une participation multipartite au dialogue institutionnel régulier, l'Irlande est convaincue que celui-ci permettra de se concentrer davantage sur l'aide à apporter aux États pour mettre en œuvre le cadre de comportement responsable ainsi que sur le renforcement des capacités en fonction des besoins afin d'accroître la cyberrésilience.

Aux fins de la mise en place d'un dialogue institutionnel régulier pleinement opérationnel avant la fin du mandat du groupe de travail à composition non limitée, l'Irlande encourage celui-ci à organiser des réunions intersessions et des sessions spéciales en 2024 et 2025, y compris sur les incidences budgétaires.

Japon

[Original : anglais]
[30 avril 2024]

1. Introduction

Le Japon est favorable à l'élaboration, en tant que mécanisme futur, d'un programme d'action destiné à promouvoir le comportement responsable des États dans le cyberespace. 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 composition non limitée à l'issue de son mandat. Il sera établi une fois le mandat de l'actuel groupe de travail à composition non limitée 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.

La présente contribution est une mise à jour de la contribution nationale du Japon figurant dans le rapport publié sous la cote A/78/76. Elle tient compte des avancées permises par la résolution 78/16 de l'Assemblée générale et des débats qui se sont poursuivis au sein du groupe de travail à composition non limitée (2021-2025).

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 :

i) Fournir des recommandations pour orienter les mesures prises au niveau national en vue d'appliquer les normes et principes de comportement responsable des États ;

ii) Encourager la communication, à titre volontaire, d'informations sur les pratiques nationales afin de recenser les besoins et les difficultés de chaque État Membre ;

iii) Appuyer, à la demande des pays bénéficiaires, les initiatives de renforcement des capacités, lesquelles sont adaptées aux besoins et aux difficultés des pays ;

iv) 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 matière de renforcement des capacités. Cet exercice devrait faciliter la mise en place d'un cadre destiné à appuyer les pratiques appliquées 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 réunions plénières ordinaires, annuelles ou semestrielles, à l'ONU, dans le cadre desquelles on adopterait et mettrait à jour régulièrement des recommandations concrètes concernant les efforts de mise en œuvre déployés au niveau national. Par exemple, on pourrait, à l'occasion d'une réunion plénière, 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 ou des réunions ou groupes de travail techniques à composition non limitée, qui se réuniraient à l'occasion de réunions intersessions tenues dans le cadre des réunions plénières du programme d'action et qui présenteraient leurs conclusions aux réunions plénières suivantes.

En complément des débats sur l'évolution du cadre, des conférences d'examen seront organisées dans le cadre du programme d'action à une fréquence devant être déterminée, l'idée étant de tenir compte de l'évolution rapide de la technologie et de veiller à ce que le cadre ne devienne pas un fardeau, en particulier pour les délégations des pays en développement.

Le répertoire mondial d'interlocuteurs, établi par l'actuel groupe de travail à composition non limitée, 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 cyberespace, 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 par la création d'un système de communication de l'information qui lui serait propre, soit par un mécanisme existant (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). Les informations communiquées aideront à recenser les priorités à suivre pour mettre en œuvre le cadre et à définir les besoins en matière de renforcement des capacités.

Les réunions plénières relatives au programme d'action pourraient porter sur les moyens d'approfondir la question de l'application du droit international dans le cyberespace. 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 cyberespace. Dans le cadre de cet axe de travail, et conformément à leur mandat, les États Membres pourraient échanger leurs vues et mener des débats reposant sur des scénarios. Pareil axe de travail porterait sur des questions générales, des concepts précis du droit international ou des sujets thématiques, tels que les cyberopérations visant des infrastructures critiques, tout en couvrant les principes pertinents du droit international.

d) Participation multipartite

Les parties prenantes sont au cœur du cyberespace, que ce soit en tant que propriétaires et exploitants d'éléments de l'infrastructure ou en tant que porte-parole des communautés. Compte tenu de la nature interconnectée du cyberespace, il est essentiel d'associer les diverses parties prenantes au débat tenu dans le cadre de l'ONU.

Le programme d'action permettrait de dialoguer et de collaborer avec la communauté des parties prenantes, notamment pour optimiser les activités de renforcement des capacités.

4. Travaux préparatoires et modalités d'établissement du futur mécanisme

Le Japon est favorable à la tenue de nouvelles discussions ciblées au sein du groupe de travail à composition limitée (2021-2025) afin de poursuivre l'élaboration du futur mécanisme.

Lettonie

[Original : anglais]
[30 avril 2024]

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 de l'Assemblée générale et fait l'objet de débats dans le cadre de plusieurs Groupe d'experts gouvernementaux et de groupes de travail à composition non limitée, ce qui souligne l'importance croissante de l'utilisation responsable du numérique aux fins du maintien de la stabilité et de la sécurité internationales. Il est essentiel que les États coopèrent pour lutter efficacement contre les menaces croissantes dans le cyberespace et renforcer la confiance entre eux. Pour ces raisons, il est temps de décider de la mise en place d'un mécanisme permanent au sein des Nations Unies pour traiter les questions de cybersécurité à long terme.

Les cyberattaques sont de plus en plus sophistiquées et destructrices et se font de plus en plus fréquentes dans notre monde moderne et interconnecté. Le paysage cybernétique est en constante évolution. Les cyberattaques contre les infrastructures critiques, les attaques motivées par des considérations politiques, les attaques par logiciels rançonneurs et l'utilisation malveillante de l'intelligence artificielle s'intensifient. Il est donc indéniable que la cybersécurité revêt un intérêt particulier dans le débat sur la sécurité internationale.

Pour faire face au niveau sans précédent d'activités malveillantes dans le cyberespace, la Lettonie renforce sa propre cybersécurité et sa résilience. Elle organise et mène notamment des opérations de chasse aux cybermenaces tant au niveau national qu'au sein de l'Union européenne, et ses institutions gouvernementales partagent leurs connaissances et leurs données d'expérience avec les citoyens et les entités publiques et privées. En 2023 et 2024, la Lettonie, ainsi que d'autres États membres de l'Union européenne, a condamné publiquement à plusieurs reprises les cyberactivités malveillantes, notamment les cyberattaques visant les processus et institutions démocratiques.

La proposition tendant à établir un « dialogue institutionnel régulier » sous les auspices de l'Organisation des Nations Unies a déjà fait l'objet de débats au sein de la Première Commission et a été mentionnée dans le rapport final du groupe de travail à composition non limitée (2019-2021)[39]. Celui-ci 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 »[40]. Dans le rapport annuel de 2023 du groupe de travail à composition non limitée (2021-2025), les États sont convenus des éléments communs, notamment un mécanisme permanent à voie unique, dirigé par les États[41].

[39] Rapport final du groupe de travail à composition non limitée (2019-2021), par. 68 à 74.
[40] Ibid., par. 74.
[41] Deuxième rapport annuel du groupe de travail à composition non limitée (2021-2025) (A/78/265), par. 55 a).

Face à la multiplication des cybermenaces, les États doivent consacrer leur énergie et leurs ressources au renforcement de la coopération et de la confiance entre les États à long terme plutôt qu'à des débats sur les modalités d'un nouveau mécanisme se déroulant tous les deux ou trois ans et risquant de fragmenter les progrès à venir. La Lettonie, en tant que petit État, est favorable à une approche à voie unique qui faciliterait l'utilisation efficace de ressources limitées.

Un programme d'action a été proposé comme suite à l'appel lancé en faveur de la mise en place d'un mécanisme permanent visant à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le cadre d'une stratégie cohérente et à long terme[42]. Les résolutions 77/37[43] et 78/16[44] relatives au programme d'action, adoptées en 2022 et 2023, respectivement, ont reçu un large soutien de la part des États à l'Assemblée générale. Le programme a été élaboré de manière transparente, inclusive et progressive.

Programme d'action en tant que mécanisme permanent des Nations Unies

La Lettonie pense que, par ses résolutions 77/37 et 78/16, l'Assemblée générale a accordé un mandat robuste pour procéder à la mise en place du programme d'action. Celui-ci constituerait un mécanisme permanent, inclusif et orienté vers l'action au sein de la Première Commission, qui serait dirigé par les États, ainsi qu'une plateforme à laquelle tous les États pourraient participer. Son objectif primordial serait de contribuer au renforcement de la paix et de la sécurité internationales et à la prévention des conflits et des malentendus entre les États. Le programme d'action porterait sur les questions liées à l'utilisation du numérique conformément au droit international et à l'application du cadre de comportement responsable des États dans le cyberespace. Comme indiqué dans la résolution 77/37 de l'Assemblée générale, le programme d'action devrait « tenir compte des conclusions adoptées par consensus »[45] par le groupe de travail à composition non limitée (2021-2025).

Il sera possible de renforcer la stabilité et la sécurité dans le cyberespace en appuyant la mise en œuvre et l'amélioration, selon qu'il convient[46], d'un cadre de comportement responsable des États fondé sur le droit international, y compris la Charte des Nations Unies dans son intégralité. Comme indiqué dans les rapports du Groupe d'experts gouvernementaux établis en 2013, 2015 et 2021 et les rapports du groupe de travail à composition non limitée établis en 2021 et 2022, le droit international, y compris le droit international humanitaire, est applicable au cyberespace et est essentiel au maintien de la paix, de la sécurité et de la stabilité dans cet espace.

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 et fondées sur les besoins menées à cette fin. Il importe de collaborer davantage en matière de renforcement des capacités et de partager nos données d'expérience et nos meilleures pratiques afin d'améliorer la résilience face aux cybermenaces aux niveaux national et mondial.

---

[42] https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf (en anglais).

[43] 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 ».

[44] Résolution 78/16 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 ».

[45] Résolution 77/37 de l'Assemblée générale, par. 2.

[46] Résolution 76/19 de l'Assemblée générale, par. 10 du préambule.

On pourrait, dans le cadre du programme d'action, tenir des sessions formelles annuelles et, entre ces sessions, organiser les travaux au sein de groupes de travail techniques consacrés à des questions spécifiques. Par exemple, un groupe de travail technique pourrait s'efforcer de mieux comprendre comment le droit international s'applique à l'utilisation du numérique. Les recommandations formulées par les groupes de travail techniques seraient adoptées aux sessions formelles. Les autres priorités définies dans le cadre du programme d'action devraient être examinées périodiquement lors des conférences d'examen.

Les groupes techniques pourraient être créés et clôturés par les décisions prises aux sessions annuelles. Ils doivent être inclusifs et ouverts à tous les États et garantir la participation des expertes et experts nationaux en présentiel ou en ligne (format hybride). Les décisions relatives aux groupes techniques et à leurs modalités de travail devraient être prises en tenant compte des capacités et des ressources des petits États.

Il est essentiel d'engager un dialogue régulier et véritable, facilité par le programme d'action, avec les parties prenantes issues de la société civile, du secteur privé et des milieux universitaires, dont les compétences spécialisées dans le domaine en constante évolution de la cybernétique sont inestimables et dont les contributions aident à promouvoir le comportement responsable des États. Les parties prenantes elles-mêmes ont également « 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 », car ce sont elles qui sont à l'origine du développement des nouvelles technologies[47].

D'autres discussions ciblées devraient être organisées en 2024 et 2025 dans le cadre des sessions restantes et des réunions intersessions du groupe de travail à composition non limitée (2021-2025) afin de continuer à préciser les différents aspects du programme d'action, notamment les modalités de sa mise en place. Le programme d'action devrait être prêt à l'issue des travaux du groupe de travail à composition non limitée (2021-2025).

Nouvelle-Zélande

[Original : anglais]
[30 avril 2024]

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.

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 cyberespace, lequel a été approuvé par l'Assemblée générale et repose sur quatre piliers :

- Droit international : tous les États Membres de l'ONU conviennent que le droit international s'applique au comportement des États dans le cyberespace ;
- 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 ;

[47] Rapport final du groupe de travail à composition non limitée (2019-2021), par. 10.

- 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.

La Nouvelle-Zélande approuve sans réserve la décision prise par l'Assemblée générale dans sa résolution 78/237 de créer, à l'issue des travaux du groupe de travail à composition non limitée (2021-2025) et au plus tard en 2026, un mécanisme placé sous l'égide de l'Organisation des Nations Unies, lequel sera permanent, inclusif et orienté vers l'action et aura pour objectifs ceux énoncés dans sa résolution 77/37 et les éléments communs pour un futur dialogue institutionnel régulier établis par consensus dans le rapport d'activité annuel de 2023 du groupe de travail à composition non limitée (2021-2025).

La Nouvelle-Zélande envisage ce mécanisme comme le « foyer permanent » des discussions sur la cybersécurité à l'ONU à l'issue des travaux de l'actuel groupe de travail à composition non limitée (2021-2025), qui s'appuierait sur la proposition adoptée dans les résolutions 77/37 et 78/237. Elle salue et appuie la résolution présentée par la France, au nom d'un groupe interrégional, qui offre à tous les États une solution claire et transparente pour examiner la portée, la structure, la teneur et les modalités du futur mécanisme de manière complémentaire à l'actuel groupe de travail à composition non limitée. À cet égard, elle soutient la mise en place d'un programme d'action :

a) Qui soit un mécanisme unique et 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 cyberespace, notamment dans le respect du droit international et des obligations internationales leur incombant en matière de droits humains, et qui, ainsi, s'appuie sur les travaux fondamentaux des groupes d'experts gouvernementaux et des groupes de travail à composition non limitée 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 cyberespace), 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 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 les mesures pratiques à prendre pour promouvoir le cadre de comportement responsable des États ainsi que sur les mesures de renforcement des capacités qui aident les États à mettre en œuvre le cadre et les mécanismes de responsabilité et de contrôle ;

e) Qui soit flexible et adaptable, de sorte à faire face aux nouvelles menaces.

Pays-Bas (Royaume des)

[Original : anglais]
[1er mai 2024]

Introduction

Les Pays-Bas restent profondément préoccupés par le risque croissant que représente l'utilisation malveillante des technologies de l'information et des communications 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 des personnes. 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, les Pays-Bas 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, dont l'Assemblée générale s'est félicitée dans ses résolutions 77/37 et 78/16.

Conformément au paragraphe 8 de la résolution 78/237 intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », les Pays-Bas présentent leurs vues et évaluations sur la sécurité du numérique et de son utilisation, en particulier sur le futur dialogue institutionnel régulier relatif à ces questions sous les auspices de l'Organisation des Nations Unies. Les vues présentées ci-après s'inscrivent dans le prolongement de la communication présentée par les Pays-Bas, en application de la résolution 77/37, aux fins de l'établissement du rapport du Secrétaire général (A/78/76).

Dans le cadre du groupe de travail à composition non limitée (2021-2025), des progrès considérables ont été faits s'agissant de trouver un terrain d'entente sur le futur mécanisme de dialogue institutionnel régulier sur la sécurité en matière d'utilisation des technologies numériques. À cet égard, les Pays-Bas se félicitent des éléments communs au sujet du dialogue institutionnel régulier qui figurent dans le rapport d'activité annuel de 2023 du groupe de travail à composition non limitée. Les Pays-Bas restent déterminés à faire de nouveaux progrès sur cette question dans le cadre du groupe de travail à composition non limitée (2021-2025).

Portée et objectifs

Réaffirmant le paragraphe 4 de la résolution 78/16 de l'Assemblée générale, les Pays-Bas estiment qu'il convient de créer, à l'issue des travaux du groupe de travail à composition non limitée (2021-2025) et au plus tard en 2026, un mécanisme placé sous l'égide de l'Organisation des Nations Unies, lequel sera permanent, inclusif et orienté vers l'action et aura pour objectifs ceux énoncés dans sa résolution 77/37 et les éléments communs pour un futur dialogue institutionnel régulier établis par consensus dans le rapport d'activité annuel de 2023 du groupe de travail à composition non limitée (2021-2025).

Les Pays-Bas soutiennent l'initiative visant à établir, sous l'égide de l'Organisation des Nations Unies, un programme d'action destiné à promouvoir le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale. Le programme d'action devrait s'appuyer sur les éléments communs pour un futur dialogue institutionnel régulier établis par consensus dans le rapport d'activité annuel de 2023 du groupe de travail à composition non limitée (2021-2025) et les décisions relatives à la portée, à la structure, aux composantes et aux modalités du programme devraient être définies sur la base des conclusions adoptées par consensus par le groupe de travail à composition non limitée.

Structure et modalités

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. Le mandat du programme d'action pourrait découler d'un document fondateur, dans lequel les États affirmeraient leur engagement à respecter le cadre de comportement responsable dans le cyberespace, et par lequel serait établi un mécanisme permettant d'avancer dans la réalisation de ses objectifs.

Le programme d'action doit être ouvert à la participation de tous les États Membres, des observatrices et observateurs permanents, des organisations intergouvernementales et autres et des institutions spécialisées. Si les États sont responsables au premier chef du maintien de la paix et de la sécurité internationales, le programme devrait également permettre la participation véritable, 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 :

a) De conférences d'examen périodiques visant à examiner l'évolution du contexte dans lequel les menaces pesant sur le cyberespace apparaissent ainsi que les initiatives menées dans le cadre du programme d'action, de sorte à actualiser le cadre selon les besoins et à fournir une orientation stratégique ;

b) De discussions plénières ouvertes visant à examiner les menaces nouvelles et existantes, à étudier plus avant l'application du droit international, à débattre de l'application de mesures de confiance, à recenser les priorités en matière de renforcement des capacités, à examiner la mise en œuvre des normes, règles et principes et à donner des orientations en ce qui concerne les réunions techniques à participation non limitée et les initiatives concrètes ;

c) De réunions techniques à participation non limitée ou de groupes de travail à composition non limitée, dans le cadre desquels on tiendrait des débats orientés vers l'action, ouverts à la participation des parties prenantes concernées et consacrés à des questions spécifiques.

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

La résolution 78/16, la résolution 77/37 et le rapport du Secrétaire général (A/78/76) fournissent une première feuille de route pour la mise en place du programme d'action. En 2025-2026, à l'issue des travaux du groupe de travail à composition non limitée, 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, afin d'adopter le document fondateur ou la déclaration politique.

Renforcement des capacités dans un futur mécanisme

Sans préjudice des conclusions du groupe de travail à composition non limitée et des décisions prises par l'Assemblée générale en ce qui concerne la mise en place d'un futur mécanisme, les Pays-Bas proposent les éléments ci-après afin de faciliter le renforcement des capacités touchant le cyberespace, l'idée étant de faire progresser la mise en œuvre du cadre évolutif et cumulatif et de promouvoir la coopération internationale à cet égard. Cette proposition s'articule autour d'un cycle en quatre étapes consistant à :

a) échanger sur les menaces en mettant en commun les compétences techniques et en examinant les moyens de faire face à ces menaces sous l'angle du cadre de comportement responsable des États dans le cyberespace adopté par consensus ;

b) recenser les besoins propres en matière de capacités dans le cadre de la communication volontaire d'informations au regard du cadre cumulatif et évolutif visant à promouvoir le comportement responsable des États. Les méthodes existantes de communication volontaire d'informations peuvent être utilisées, comme l'enquête de l'Institut des Nations Unies pour la recherche sur le désarmement (initiative mexico-australienne) 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 ;

c) faire correspondre les besoins et les ressources. Le futur mécanisme pourrait servir de cadre de rencontre. En outre, compte tenu du caractère universel et de la réputation de l'ONU, le Secrétariat pourrait faciliter la coordination des travaux des organisations et des structures en matière de renforcement des cybercapacités. Le futur mécanisme pourrait s'appuyer sur des outils existants tels que le portail Cybil du Forum mondial sur la cyber expertise et, potentiellement, sur des propositions actuellement examinées par le groupe de travail à composition non limitée (2021-2025), telles que le catalogue de renforcement des capacités et le portail mondial de coopération en matière de cybersécurité proposés par les États Membres ;

d) mettre en place un système de retour d'informations permettant aux États d'échanger leurs données d'expérience en ce qui concerne leurs activités de mise en œuvre et de renforcement des cybercapacités, ce qui pourrait éclairer d'autres débats sur l'utilisation du numérique par les États dans le contexte de la sécurité internationale.

Les activités de renforcement des capacités menées dans le cadre du futur mécanisme devraient être entreprises conformément aux principes convenus dans le rapport d'activité annuel de 2023 du groupe de travail à composition non limitée.

Singapour

[Original : anglais
1er mai 2024]

Singapour reste attachée à un débat mondial ouvert et inclusif sur la cybersécurité, et c'est à cet égard qu'elle considère qu'il est extrêmement important que tous les États s'engagent envers un futur dialogue institutionnel régulier et unique. Un tel dialogue est essentiel aux fins de l'acceptation et de la reconnaissance universelles du cadre cumulatif et évolutif de comportement responsable des États dans l'utilisation des technologies de l'information et des communications, convenu par tous les États Membres de l'Organisation des Nations Unies depuis 1998, et à la création d'une plateforme mondiale commune aux fins de la poursuite du développement et de la mise en œuvre de ce cadre. À cet égard, il est crucial que tous les États puissent concentrer leurs efforts sur un processus unique afin que les

discussions continuent de porter sur le fond et ne soient pas fragmentées. De plus, les petits États et les États en développement disposant de ressources limitées ne seraient pas en mesure de participer durablement à des processus parallèles doubles.

Singapour estime qu'il faudrait continuer à utiliser les quatre éléments communs du dialogue institutionnel régulier convenus dans le deuxième rapport d'activité annuel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) (A/78/265, par. 55) pour instaurer la confiance nécessaire à un consensus sur un mécanisme permanent à voie unique.

Il est important que les États utilisent le peu de temps et d'espace qu'il leur reste pour travailler à l'élaboration d'une vision commune de la voie à suivre pour un dialogue institutionnel régulier au sein de l'actuel groupe de travail à composition non limitée. La priorité doit être donnée à la recherche d'un consensus. À cet égard, Singapour soutient la proposition faite par le Brésil à la septième session de fond du groupe de travail à composition non limitée, qui portait sur l'instauration d'un moratoire sur la présentation de résolutions relatives à la sécurité du numérique à la Première Commission de l'Assemblée générale jusqu'à ce que l'actuel groupe de travail à composition non limitée achève ses travaux en 2025. Nous soutenons la présidence du groupe de travail à composition non limitée dans la poursuite des discussions sur la voie à suivre pour un dialogue institutionnalisé régulier, en vue de développer et d'affiner une proposition de consensus pour un tel dialogue.

Nous pensons que, dans un deuxième temps, il serait utile que le groupe de travail à composition non limitée actuel se mette d'accord sur le champ d'application, la structure, les objectifs et la fréquence des réunions du futur mécanisme. Répondre à ces questions pratiques est un moyen logique de s'appuyer sur les éléments communs sur lesquels tous les États sont déjà parvenus à un consensus. Les délégations, en particulier les petites délégations disposant de ressources limitées, auront ainsi une vision claire de leurs travaux après 2025 et pourront commencer la planification nécessaire pour optimiser leur participation de manière significative. Afin de garantir une base durable pour un mécanisme universel permanent à voie unique, Singapour souligne également que la conception du futur mécanisme doit être suffisamment large et flexible pour faciliter les discussions continues et futures sur les propositions et les priorités de toutes les délégations. En particulier, il serait utile de réexaminer périodiquement le fonctionnement du mécanisme permanent afin de vérifier que ses travaux sont adaptés à l'évolution constante des menaces opérationnelles. À cet égard, Singapour soutient l'approche et la structure présentées dans le document de travail communiqué par le Président le 20 février 2024 et portant sur les projets d'éléments pour le mécanisme permanent. Singapour se réjouit de travailler de manière constructive avec toutes les délégations pour affiner ces projets d'éléments en vue de leur adoption par consensus dans le troisième rapport d'activité annuel de l'actuel groupe de travail à composition non limitée.

Tchéquie

[Original : anglais]
[30 avril 2024]

La Tchéquie est pleinement déterminée à faire progresser le débat mondial sur la cybersécurité à l'Organisation des Nations Unies et se félicite des progrès réalisés jusqu'à présent par les groupes de travail à composition non limitée et les groupes d'experts gouvernementaux de l'ONU.

L'une des principales réalisations du groupe de travail à composition non limitée et du Groupe d'experts gouvernementaux est d'avoir élaboré et consolidé un cadre de comportement responsable des États dans le cyberespace.

À cet égard, la Tchéquie estime que la mise en œuvre du cadre de comportement responsable des États dans le cyberespace devrait être le thème central du futur dialogue institutionnel. En outre, elle appuie la création d'un mécanisme permanent, à voie unique, inclusif et orienté vers l'action sous l'égide de l'ONU à la fin de l'actuel groupe de travail à composition non limitée en 2025.

Parallèlement, la Tchéquie juge que pour établir un futur dialogue institutionnel qui fonctionnerait efficacement dans l'intérêt de tous, il importe de poursuivre le débat sur sa forme concrète dans l'actuel groupe de travail. À l'heure actuelle, la communauté internationale dispose d'un peu plus d'un an pour mener ce débat.

En ce qui concerne le débat au sein du groupe de travail à composition non limitée, la Tchéquie souhaite appeler votre attention sur le fait que la proposition la plus élaborée, la plus débattue et la plus consensuelle en vue d'un futur dialogue institutionnel est le programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique.

En revanche, la Tchéquie estime que la résolution 78/237, intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », ne reflète pas l'approche progressive adoptée par le groupe de travail à composition non limitée ni le consensus auquel il est parvenu ces dernières années. Elle semble privilégier les intérêts d'un groupe restreint d'États.

Le débat sur le programme d'action se poursuit sans interruption depuis 2020 et la Tchéquie y participe activement. Elle constate que les débats en cours au groupe de travail à composition non limitée au sujet du programme d'action sont utiles, car ils ont permis de définir l'orientation du programme d'action et de clarifier plusieurs points qui pourraient prêter à controverse. La Tchéquie estime qu'il est important de poursuivre ces échanges afin d'arrêter le contenu et les modalités du futur mécanisme. À la lumière de ce qui précède, elle suggère que des réunions intersessions et des sessions spéciales du groupe de travail à composition non limitée soient organisées en 2024 et 2025 afin de se concentrer sur des aspects particuliers du programme d'action, y compris sur ses incidences budgétaires.

En outre, la Tchéquie souhaite appeler l'attention sur certains éléments du programme d'action qui sont ressortis des débats, et qu'elle estime être les principaux atouts du programme d'action.

- 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 au domaine cyber à l'ONU. Ainsi, on éviterait des débats récurrents sur la création d'un nouveau groupe de travail consacré à l'utilisation du numérique.

- Le programme d'action appuierait la mise en œuvre du cadre de comportement responsable des États et permettrait de poursuivre le débat sur l'élaboration de ce cadre, le cas échéant.

- Le programme d'action permettrait de mettre en application les principes de renforcement des capacités via ses objectifs orientés vers l'action et de favoriser leur mise en œuvre dans des projets de renforcement des capacités cyber. Dans le cadre de ce programme d'action, on pourrait tirer parti des activités en cours ou potentielles visant à renforcer les capacités, et accroître leur visibilité tout en améliorant leur coordination. Par exemple, on pourrait envisager la coordination

avec les activités de renforcement des capacités cybernétiques entreprises par d'autres instances telles que l'Union internationale des télécommunications.

- Le programme d'action faciliterait une participation et une collaboration constructives avec les parties prenantes non gouvernementales. 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 programme d'action est conçu pour servir de cadre global, qui pourrait inclure d'autres initiatives qui ont été examinées ou approuvées dans le cadre du groupe de travail à composition non limitée.

En ce qui concerne les modalités précises, la Tchéquie penche pour des sessions plénières annuelles et des réunions des groupes de travail techniques spécialisés pendant l'intersession.

- La création et la suppression d'un groupe de travail particulier relèveraient entièrement de la compétence des États.
- La portée et les travaux préparatoires de ces débats techniques se limiteraient aux thèmes retenus aux sessions plénières, et un nombre restreint d'experts des gouvernements et, le cas échéant, d'autres parties prenantes telles que les acteurs des milieux universitaires, par exemple, y participeraient. En particulier, ces groupes de travail pourraient se concentrer sur des sujets tels que la protection des infrastructures critiques, la réponse aux cyberincidents, et l'applicabilité de dispositions concrètes sur des questions précises relevant du droit international dans le cyberespace.
- La Tchéquie juge que si tout est bien organisé, la création de groupes de travail techniques intersessions peut accroître considérablement l'efficacité des travaux et alléger la charge de travail des différentes délégations.
- Il pourrait être utile d'envisager de ne pas tenir toutes les réunions des groupes de travail intersessions à New York, mais d'examiner également d'autres lieux.

Türkiye

[Original : anglais
1er mai 2024]

Les technologies de l'information et des communications sont devenues un élément incontournable de la société et de l'économie et sont omniprésentes dans le quotidien de chacun. Elles sont utilisées dans de nombreux domaines, tant par les particuliers que par les États. Aujourd'hui, les compétences des États en matière de développement et d'utilisation des technologies jouent un rôle important dans le développement et la croissance. Les technologies de l'information sont devenues le principal facteur de développement dans presque tous les domaines : transports, communications, industrie de la défense, sciences médicales, appareil productif, éducation, commerce, etc.

Des études indiquent que les tendances liées aux technologies vont s'accélérer au cours des prochaines années. Dans ce contexte, les acteurs qui se distinguent sont ceux qui parviennent à établir de nouvelles normes technologiques, à faire éclore de nouveaux secteurs d'activité ou à modifier en profondeur des secteurs existants. L'Internet des objets, la 5G, les mégadonnées, la technologie de la chaîne de blocs,

l'intelligence artificielle, les véhicules autonomes et les robots intelligents sont considérés comme des technologies qui vont éclairer notre présent et notre avenir.

Si ces technologies offrent de nombreuses possibilités, elles s'accompagnent toutefois également de risques liés à la cybersécurité. Les cybermenaces prennent des formes de plus en plus complexes et leur nombre augmente de jour en jour. Selon une étude, il y aurait eu plus de 493 millions de tentatives d'extorsion par logiciel rançonneur dans le monde en 2022[48].

Il n'y a donc d'autre choix que de se préoccuper des questions de cybersécurité à chaque étape pour que le développement et l'intégration des technologies se fassent en toute sécurité. Les failles de sécurité dans les systèmes d'information et de communication peuvent entraîner la mise hors service ou l'utilisation à des fins illicites de ces systèmes, la perte de vies humaines, des dommages économiques de grande ampleur, la perturbation de l'ordre public et la violation de la sécurité nationale.

La cybersécurité n'est pas seulement indispensable pour se préserver des menaces dans les domaines où la technologie est omniprésente ; c'est aussi un facteur important pour le bien-être et la sécurité des pays en raison des risques que l'usage des technologies fait peser sur le cours de la vie sociale et économique. Au vu de ces évolutions, les pays investissent des sommes très importantes dans le domaine de la cybersécurité, développent des technologies de cybersécurité et orientent leur action pour assurer leur sécurité dans le cyberespace et accroître leur résistance aux attaques.

La lutte contre les cybermenaces est considérée comme une question de politique nationale dans notre pays. Dans ce contexte, des études portant sur la cybersécurité nationale sont menées par le Ministère des transports et des infrastructures au niveau stratégique et par l'Autorité des technologies de l'information et des communications au niveau technique. D'autres institutions et organisations participent également à ces études.

Les études menées depuis 2012 ont débouché sur l'élaboration et la mise en application de stratégies nationales de cybersécurité assorties de plans d'action. Conformément aux dispositions de la dernière stratégie nationale de cybersécurité en date et du plan d'action correspondant, élaborés pour la période 2020-2023, des études ont été menées pour assurer la cybersécurité des infrastructures critiques 24 heures sur 24 et sept jours sur sept, renforcer les compétences des équipes d'intervention en cas de cyberincident, rendre le cyberespace plus sûr pour toutes les sphères de la société, continuer à bien faire connaître les risques liés à la cybersécurité, partager des informations et coopérer avec les parties prenantes nationales et internationales, et mettre en place des mécanismes de protection, de lutte contre la cybercriminalité et de dissuasion.

En outre, le Ministère des transports et des infrastructures a entamé des études en vue d'élaborer une nouvelle stratégie de cybersécurité et un nouveau plan d'action pour la période 2024-2028. Les études se poursuivent donc en vue d'assurer une coopération efficace entre toutes les parties prenantes, d'intensifier l'acquisition, la production et le partage de renseignements sur les cybermenaces, d'augmenter le niveau de préparation du pays aux cyberincidents, de développer des compétences spécialisées, de mettre au point des mécanismes de détection rapide et de réaction précoce et d'effectuer des analyses de risques relatives aux secteurs et infrastructures critiques.

L'équipe nationale d'intervention informatique d'urgence, qui relève de l'Autorité des technologies de l'information et des communications, coordonne la

[48] www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide.

réponse apportée par la Türkiye aux cyberincidents depuis 2013. Elle est chargée de la détection des cybermenaces et de la réponse aux cyberincidents, y compris avant, pendant et après les faits, mais aussi des mesures préventives et de la cyberdissuasion.

Ses principaux domaines d'intervention sont les suivants :

- renforcement des capacités cyber ;
- adoption de mesures technologiques ;
- collecte et diffusion de renseignements sur les menaces ;
- protection des infrastructures critiques.

Dans l'intérêt de la cybersécurité du pays, 14 équipes sectorielles d'intervention spécialisées dans certains secteurs ou infrastructures critiques (énergie, santé, banque et finance, gestion de l'eau, communications électroniques et services publics critiques) et plus de 2 200 équipes institutionnelles d'intervention en cas d'atteinte à la sécurité informatique ont également été créées depuis 2013. Toutes ces équipes, actives 24 heures sur 24 et sept jours sur sept, sont chapeautées par l'équipe nationale d'intervention informatique d'urgence et ont pour mission de réduire les risques informatiques et de lutter contre les cybermenaces. L'équipe nationale d'intervention informatique d'urgence utilise des outils de détection et de prévention à des fins de surveillance, et des outils de notification pour partager des informations avec les parties concernées. Elle a développé la plateforme de partage d'informations commune à toutes les équipes d'intervention en cas d'atteinte à la sécurité informatique en Türkiye afin de diffuser des alarmes, des avertissements et des avis de sécurité, ce qui constitue un canal de communication efficace et sécurisé.

Les exercices de cybersécurité sont une autre activité importante de coopération et de préparation. Ces types d'exercices réalisés au niveau national et international contribuent à renforcer le cyberespace et à mettre à l'essai les mesures à prendre contre les cybermenaces potentielles. Depuis 2011, le Ministère des transports et des infrastructures a organisé sept exercices nationaux et deux exercices internationaux de cybersécurité. Plus récemment, en 2022, des exercices nationaux de cybersécurité Cyber Shield ont été organisés. Après ces exercices, une manifestation placée sous le thème « Cyber Shield 2022 pour le secteur financier » a été organisée les 20 et 21 octobre 2022 avec la coopération du Ministère des transports et des infrastructures et de l'Autorité des technologies de l'information et des communications et avec la participation d'institutions et d'organisations publiques. Au cours de ces exercices, grâce à l'infrastructure technique et aux scénarios mis au point par l'équipe nationale d'intervention informatique d'urgence, les participants ont pu acquérir une expérience pratique de la cybersécurité et être informés des mesures à prendre en cas de cyberattaques. Il est prévu d'organiser un exercice international de cybersécurité dans la période à venir.

La cybersécurité est une préoccupation dans le monde entier et doit faire l'objet d'initiatives menées au niveau international. La coopération aux niveaux régional et mondial et le partage d'informations et de renseignements dans le domaine de la cybersécurité ont une forte incidence sur la capacité des pays à faire face aux risques et aux menaces cyber. C'est pourquoi la Türkiye mène une coopération bilatérale, régionale et internationale dans ce domaine et participe et contribue aux activités d'élaboration de politiques et de stratégies menées par des organisations internationales telles que l'Organisation des Nations Unies, l'Organisation du Traité de l'Atlantique Nord (OTAN), l'Organisation pour la sécurité et la coopération en Europe, le Groupe des 20, l'Organisation de coopération et de développement économiques, l'Organisation de coopération économique, le groupe des huit, le Centre pour la coopération de sécurité et l'Organisation des États de langue turcique,

entre autres. En outre, l'équipe nationale d'intervention informatique d'urgence poursuit ses activités de partage de renseignements sur les cybermenaces dans le cadre de plateformes internationales auxquelles elle appartient, telles que le Forum of Incident Response and Security Teams, Trusted Introducers, l'Union internationale des télécommunications, la Cybersecurity Alliance for Mutual Progress, la Plateforme multinationale d'échange d'informations sur les logiciels malveillants de l'OTAN, et l'équipe d'intervention informatique d'urgence de l'Organisation de la coopération islamique. La Türkiye participe également aux activités du Centre d'excellence pour la cyberdéfense en coopération de l'OTAN en tant que pays parrain et contribue à la capacité d'aide à distance en cas d'incident cyber (VCISC) mise en place par cette organisation. En outre, des mémorandums d'accord et des accords de coopération bilatérale en matière de cybersécurité ont été signés avec de nombreux pays.

L'équipe nationale d'intervention informatique d'urgence ayant intégré le programme CVE (Common Vulnerabilities and Exposures) de l'organisme MITRE, elle attribue des numéros d'identifiant aux vulnérabilités de logiciels, de matériels et de produits d'entreprises extérieures, et elle coordonne la gestion de ces vulnérabilités.

La Türkiye est partie à plusieurs accords multilatéraux en matière de cybersécurité. Elle a ratifié la Convention du Conseil de l'Europe sur la cybercriminalité (Série des traités européens n° 185). Elle a également contribué aux études menées par le Comité spécial de l'ONU 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. Elle est en outre l'un des États qui coparrainent 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, et elle soutient fermement la résolution 77/37 de l'Assemblée générale des Nations Unies et la poursuite des travaux menés afin de faire du programme d'action un mécanisme permanent, inclusif et orienté vers l'action.

1. Vue d'ensemble des dispositifs nationaux de cybersécurité en Türkiye

Les premières avancées réalisées en Türkiye dans le domaine de la sécurité informatique en général et de la cybersécurité en particulier remontent à 1991, année où les actes de cybercriminalité ont été érigés en infraction pénale en vertu de la loi n° 765[49]. Depuis, la Türkiye a franchi plusieurs grandes étapes dans divers domaines de la cybersécurité, cette dernière étant considérée comme faisant partie intégrante de la sécurité nationale. On trouvera ci-après une liste non exhaustive des mesures prises avant 2013 :

- 1999 : élaboration du plan directeur de l'infrastructure informatique nationale[50] ;
- 2002 : lancement du plan d'action de l'initiative E-Türkiye[51] ;
- 2003 : présentation du projet E-Transformation Türkiye, assorti d'un plan d'action à court terme pour la période 2003-2004[52] ;
- 2004 : adoption de la loi n° 5070[53] sur la signature électronique et de la loi n° 5237[54] du Code pénal turc ;

[49] https://www.mevzuat.gov.tr/MevzuatMetin/5.3.765.pdf.
[50] http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/991000_TuenaRapor.pdf.
[51] http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/020800_E-TurkiyeEylemPlani.pdf.
[52] https://webdosya.csb.gov.tr/db/cbs/icerikler/2005-20180522115122.pdf.
[53] https://kamusm.bilgem.tubitak.gov.tr/dosyalar/mevzuat/kanunlar/kanun.pdf.
[54] www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm#1.

- 2006 : publication de la stratégie et du plan d'action de la société de l'information pour la période 2006-2010[55] ;
- 2007 : mise en place du centre de coordination de l'équipe turque d'intervention informatique d'urgence ;
- 2007 : adoption de la loi n° 5651 sur les publications sur Internet et la lutte contre les infractions commises au moyen de ces publications[56] ;
- 2008 : entrée en vigueur de la loi n° 5809 sur les communications électroniques[57], en parallèle du premier exercice national de cybersécurité ;
- 2010 : déclaration du Conseil national de sécurité dans laquelle il reconnaît la portée mondiale des cybermenaces et le danger qu'elles représentent pour la sécurité nationale ;
- 2010 : harmonisation du droit turc avec la Convention du Conseil de l'Europe sur la cybercriminalité (Série des traités européens nº 185) ;
- 2012 : création du Conseil de la cybersécurité par le Conseil des ministres[58], conséquence de la décision par ce dernier de prendre en main et de coordonner les efforts nationaux en matière de cybersécurité, et création de l'Institut de la cybersécurité rattaché au Centre de recherche sur l'informatique et la sécurité de l'information du Conseil de la recherche scientifique et technique turc[59].

Ces mesures ont marqué des étapes importantes dans le renforcement de la cybersécurité. Comme indiqué ci-dessus, le 11 juin 2012, alors que la Türkiye était encore sous régime parlementaire, le Conseil des ministres turc a approuvé une décision sur l'exécution, la gestion et la coordination des études menées à l'échelon national dans le domaine de la cybersécurité[60], par laquelle il a créé le Conseil de la cybersécurité[61] et chargé le Ministère des transports, des affaires maritimes et des communications (devenu le Ministère des transports et des infrastructures[62]) d'en assurer le secrétariat et de coordonner les activités de cybersécurité avec les institutions concernées.

Au cours des dix dernières années, le rythme des changements dans le secteur de la cybersécurité s'est nettement accéléré en Türkiye. Parmi les grandes avancées, citons le lancement de la première stratégie nationale de cybersécurité, portant sur la période 2013-2014, et du plan d'action correspondant[63], la création du Centre national d'intervention en cas de cyberincident[64], qui relève de l'Autorité des technologies de l'information et des communications[65], et la publication d'une déclaration relative à la création, aux compétences et aux modalités de fonctionnement des équipes d'intervention en cas de cyberincident[66]. En outre, des équipes d'intervention en cas de cyberincident (équipes institutionnelles et équipes spécialisées dans certains secteurs) ont été créées au sein des institutions et organisations publiques, conformément aux dispositions énoncées dans la stratégie nationale de cybersécurité pour la période 2013-2014 et le plan d'action correspondant. Qu'elles soient

[55] http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060500_BilgiToplumuStratejisi.pdf.
[56] https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf.
[57] https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5809.pdf.
[58] www.btk.gov.tr/siber-guvenlik-kurulu.
[59] https://bilgem.tubitak.gov.tr/en/sge/.
[60] https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf.
[61] www.btk.gov.tr/siber-guvenlik-kurulu.
[62] www.uab.gov.tr/.
[63] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf.
[64] www.usom.gov.tr/.
[65] www.btk.gov.tr/.
[66] www.usom.gov.tr/hakkimizda.

rattachées à des institutions ou spécialisées dans certains secteurs, les équipes d'intervention en cas de cyberincident ont pour mission de détecter rapidement les cybermenaces et les cyberattaques et de mettre au point et de diffuser des mesures permettant de résoudre les problèmes engendrés par ces attaques. Leur objectif est donc de fournir des compétences en matière de réaction aux cyberincidents à d'autres institutions et organisations. Actuellement, 14 équipes sectorielles relevant du Centre national d'intervention en cas de cyberincident sont opérationnelles, et plus de 2 100 équipes institutionnelles travaillent avec diligence à la protection du cyberespace turc.

Le Centre de la cyberdéfense, créé au sein des forces armées turques en 2012, est devenu le Commandement de la cyberdéfense. De la même manière, le Département de lutte contre la cybercriminalité, qui avait été institué au sein de la Direction générale de la sécurité en 2011, a été restructuré en 2013.

La loi nº 6518[67], promulguée en 2014, a introduit certaines règles applicables au domaine de la cybersécurité en ajoutant des articles à la loi n° 5809 de 2008 relative à la réglementation du secteur des communications électroniques. Les articles ajoutés à la loi nº 5809 portent création d'un Conseil de la cybersécurité composé de hauts fonctionnaires et présidé par le ou la ministre des transports, des affaires maritimes et des communications. En vertu de l'alinéa h) ajouté à l'article 5 de la loi précitée, le Ministère des transports, des affaires maritimes et des communications s'est vu confier la tâche de définir des orientations, des stratégies et des objectifs pour assurer la cybersécurité nationale, de préparer des plans d'action et de mener des activités de formation et de sensibilisation aux enjeux de cybersécurité.

Ce règlement fait du Conseil de la cybersécurité la principale autorité chargée de l'approbation finale et de la mise en œuvre effective des orientations, stratégies et plans d'action nationaux établis par le Ministère des transports, des affaires maritimes et des communications. Le Conseil est également chargé de se prononcer sur les propositions relatives à la désignation des infrastructures critiques et des institutions et organisations qu'il convient d'exempter de tout ou partie des dispositions relatives à la cybersécurité.

L'année 2016 a été marquée par l'adoption de la loi nº 6698 sur la protection des données personnelles[68], de la stratégie nationale de cybersécurité pour la période 2016-2019 et du plan d'action correspondant[69], et du décret-loi nº 671[70] qui, répondant aux besoins de la période, autorise l'Autorité des technologies de l'information et des communications à prendre ou à demander que soient prises toutes sortes de mesures pour protéger les institutions et organisations publiques et les personnes physiques et morales contre les cyberattaques et pour avoir un effet dissuasif sur ces attaques. Par la suite, en 2017, la Présidence des entreprises du secteur de la défense (devenu le Secrétariat des entreprises du secteur de la défense) a coordonné la mise en place du Groupe turc de la cybersécurité, l'achèvement du processus de nomination au Conseil de protection des données personnelles et le début des activités de ce dernier[71].

En 2018, le Conseil de la cybersécurité a été dissous à la suite de l'adoption du décret-loi nº 703[72], par lequel les responsabilités et le mandat du Conseil ont été transférés à un conseil ou une autorité que le Président devait désigner. Cependant, malgré quelques nominations liées à certaines de ces responsabilités, aucune d'entre

---

[67] www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm.
[68] https://kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law.
[69] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf.
[70] www.resmigazete.gov.tr/eskiler/2016/08/20160817-18.htm.
[71] www.ssb.gov.tr/Default.aspx?LangID=2.
[72] https://www.resmigazete.gov.tr/eskiler/2018/07/20180709M3-1.pdf.

elles n'a été officiellement transférée à un conseil ou à une autorité à ce jour. Le passage au régime présidentiel a également entraîné des changements dans le processus d'élaboration de politiques. Le pouvoir de formuler des politiques a été transféré au Président de la République. Des conseils d'orientation ont été chargés de formuler et de mettre au point les politiques (décret présidentiel n° 1[73], articles 20 à 22), les ministères étant quant à eux chargés de leur application.

Depuis le 10 juillet 2018 et la mise en œuvre du premier décret adopté sous régime présidentiel, le pouvoir d'élaborer des propositions de mesures et de stratégies en matière de cybersécurité a été confié au Conseil de la sécurité et des politiques étrangères, placé sous la direction du Président (décret présidentiel nº 1, article 36/1/ğ). Le pouvoir de concevoir des projets destinés à améliorer la sécurité de l'information et la cybersécurité a quant à lui été conféré par le même décret au Département de la cybersécurité[74] du Bureau de la transformation numérique[75] rattaché à la Présidence de la République de Türkiye. Le mandat du Département comprend notamment les tâches suivantes :

- concevoir des stratégies de cybersécurité à l'intention des institutions publiques et des entreprises qui exploitent des infrastructures critiques, conformément aux orientations définies par le Président ;
- suivre les progrès réalisés afin de garantir la mise en œuvre efficace des politiques, stratégies et plans d'action nationaux en matière de cybersécurité ;
- réaliser des études visant à recenser les infrastructures critiques ;
- stimuler la coopération entre le secteur public, le secteur privé et les universités afin de développer un écosystème national de la cybersécurité ;
- réaliser des études visant à développer des produits nationaux de cybersécurité dans tous les secteurs, en particulier les secteurs liés aux infrastructures critiques, et promouvoir leur utilisation dans le secteur public ;
- organiser des activités de prévention et de protection pour sauvegarder les technologies critiques et les ressources d'information ;
- entreprendre des études sur la mise en place et la gestion des systèmes de sécurité de l'information dans les institutions publiques et les entreprises qui exploitent des infrastructures critiques ; dans ce cadre, définir des normes techniques et des procédures, ainsi que des principes régissant le suivi et le contrôle de l'application.

Le décret présidentiel nº 1, publié au Journal officiel du 10 juillet 2018, a également donné naissance à la Direction nationale de la technologie[76], placée sous l'égide du Ministère de l'industrie et de la technologie[77]. La Direction s'est vu confier les responsabilités ci-après en matière de cybersécurité :

- améliorer le niveau de maturité des produits et systèmes de cybersécurité et de sécurité de l'information et des produits et systèmes technologiques de pointe ;
- développer des produits nationaux dans le domaine de la cybersécurité ;
- répandre l'utilisation des produits nationaux dans l'ensemble du pays ;
- améliorer les infrastructures de stockage et de gestion des données ;

[73] https://www.mevzuat.gov.tr/mevzuatmetin/19.5.1.pdf.
[74] https://cbddo.gov.tr/en/.
[75] https://cbddo.gov.tr/en/department-of-cyber-security/.
[76] www.sanayi.gov.tr/merkez-birimi/c03f1f3bae27/hakkimizda.
[77] www.sanayi.gov.tr/anasayfa.

- soutenir l'écosystème de la cybersécurité au moyen de divers programmes d'incitation.

En résumé, plusieurs lois, règlements et autres textes législatifs ont désigné différentes institutions chargées de superviser la cybersécurité nationale et défini les tâches de cybersécurité attribuées à ces dernières. Comme dans la plupart des autres pays, la cybersécurité est une compétence partagée entre plusieurs entités publiques. Le Bureau de la transformation numérique et le Ministère des transports et des infrastructures ont tous deux mené des études sur l'élaboration de stratégies et de politiques en matière de cybersécurité. Ces entités ont leur propre ensemble de compétences et de responsabilités définies dans leur mandat respectif.

2. Compétences et responsabilités du Bureau de la transformation numérique en matière de cybersécurité

Le Bureau de la transformation numérique de la Présidence de la République de Türkiye a été créé le 10 juillet 2018 par la publication au Journal officiel du décret présidentiel nº 1 organisant la transition vers le régime présidentiel. Le mandat du Bureau a ensuite été élargi par le décret présidentiel n° 48 publié le 24 octobre 2019[78].

La création du Bureau a marqué une nouvelle ère et un changement d'état d'esprit concernant la transition numérique en Türkiye, amorçant une stratégie interinstitutionnelle plus cohérente et intégrée de la transformation numérique dans le secteur public. En effet, en plus de parvenir à une administration plus rapide, plus transparente et plus efficace, la mission du Bureau est de coordonner, gérer et exploiter de manière centralisée les activités de transformation numérique menées séparément par différentes institutions, en tenant compte des technologies émergentes, des demandes sociales et de l'orientation des réformes menées dans le secteur public. En outre, le Bureau a pour objectif de coordonner et de centraliser les activités liées à la cybersécurité, aux technologies nationales, aux mégadonnées et à l'intelligence artificielle, tant sur le plan stratégique que pratique, et d'assurer la mise en œuvre efficace des stratégies de haut niveau. Le Bureau est donc chargé de coordonner la définition d'objectifs macroéconomiques et la mise en œuvre d'initiatives visant à protéger les infrastructures numériques de la Türkiye, l'objectif étant de faire de cette dernière une cyberpuissance dotée d'une capacité de dissuasion dans ce domaine.

Le Bureau s'est vu confier les responsabilités ci-après dans le domaine de la cybersécurité, notamment en ce qui concerne l'élaboration de politiques, la réglementation, la création d'un écosystème de la cybersécurité, la sensibilisation du public, le renforcement des capacités, le renforcement de l'infrastructure publique et l'élaboration de normes :

- concevoir des stratégies de cybersécurité à l'intention des institutions publiques et des entreprises qui exploitent des infrastructures critiques, conformément aux orientations définies par le Président ;
- concevoir des projets visant à garantir la cybersécurité nationale et de la sécurité de l'information ;
- suivre l'évolution de la mise en œuvre effective, à l'échelle nationale, des politiques, stratégies et plans d'action en matière de cybersécurité ;
- recenser les infrastructures critiques ;

[78] https://cbddo.gov.tr/en/governance-and-responsibilities.

- faire des propositions aux agences compétentes concernant les institutions et organisations qu'il conviendrait d'exempter de tout ou partie des dispositions relatives à la cybersécurité ;
- contribuer à la création d'un écosystème national de la cybersécurité en renforçant la collaboration entre le secteur public, le secteur privé et les universités ;
- déterminer les domaines prioritaires en matière de cybersécurité afin d'orienter les capacités du secteur privé vers les domaines critiques et d'éviter les investissements redondants ;
- mettre au point, aux niveaux local et national, des produits de cybersécurité dans tous les secteurs, en particulier les secteurs liés aux infrastructures critiques, et répandre l'utilisation de ces solutions dans le secteur public ;
- réaliser des activités de prévention et de protection pour sauvegarder les technologies critiques et les ressources d'information ;
- mettre en place un système de gestion de la sécurité de l'information dans les institutions publiques et les entreprises exploitant des infrastructures critiques et en assurer le fonctionnement, en définissant des normes techniques et des procédures et des principes, et en en surveillant et facilitant l'application.

À l'heure actuelle, le Bureau est la principale autorité chargée de gérer les questions de cybersécurité pour le compte des institutions publiques et des entreprises des secteurs critiques de notre pays. En plus de faire office de conseil de la cybersécurité, il collabore avec toutes les institutions pour coordonner l'élaboration et l'exécution efficace des stratégies et plans d'action décidés à l'échelle nationale.

3. Activités et projets du Bureau de la transformation numérique concernant l'élaboration de politiques

Bien que la cybersécurité puisse être définie de différentes manières, sa définition simplifiée et générale la désigne comme la discipline qui s'intéresse à la sécurité du cyberespace en tous points, en tenant compte des différents éléments composant les technologies de l'information. Vu que l'Industrie 4.0 est une révolution qui vise à rapprocher les technologies de l'information et tous les mécanismes vitaux, nous devrions en principe intégrer les questions de cybersécurité à nos dispositifs de sécurité vitaux afin de nous adapter à cette révolution.

La mauvaise intégration de ces questions risque de poser des problèmes de sécurité et de respect de la vie privée. Parmi les objectifs stratégiques majeurs à l'échelle nationale, citons la protection des infrastructures critiques, la sécurisation du partage des données entre les institutions et les organisations et le maintien à l'intérieur du pays du trafic de données dont la source et la destination sont intérieures au pays. L'enjeu est donc d'accroître l'état de préparation aux cyberincidents aux échelles institutionnelle, sectorielle et nationale au moyen de processus d'analyse et de planification en fonction des risques.

Soucieux de garantir la sécurité du cyberespace, les pouvoirs publics élaborent et publient des stratégies de cybersécurité et en assurent l'exécution et le suivi en désignant des institutions compétentes. Notre pays remplit également son devoir à cet égard. Les travaux menés sur cette question, sous la coordination du Ministère des transports et des infrastructures, ont abouti à la publication des stratégies suivantes :

- Stratégie nationale de cybersécurité pour la période 2013-2014 et plan d'action correspondant[79] ;
- Stratégie nationale de cybersécurité pour la période 2016-2019 et plan d'action correspondant[80] ;
- Stratégie nationale de cybersécurité pour la période 2020-2023 et plan d'action correspondant[81].

Élaborés dans un souci de continuité, les stratégies nationales de cybersécurité et les plans d'action susmentionnés tendent vers une approche intégrée et prévoient des mesures à même de garantir la sûreté d'utilisation des nouvelles technologies qui font désormais partie du quotidien de chacun.

La dernière stratégie nationale de cybersécurité en date (2020-2023) et le plan d'action correspondant[82] ont été publiés le 28 décembre 2020 avec le soutien du Bureau de la transformation numérique. Cette stratégie vise à soutenir le développement économique de notre pays, à protéger la vie personnelle de nos citoyens, à sauvegarder la sécurité nationale et à faire de notre pays une référence dans le domaine de la cybersécurité. Dans cette perspective, la stratégie est axée sur des politiques quadriennales conformes à la vision et à la mission de la Türkiye en matière de cybersécurité, et vise à pousser plus loin les progrès accomplis dans le cadre des stratégies précédentes. Les objectifs stratégiques définis pour la période 2020-2023 dans le cadre de la stratégie de cybersécurité et du plan d'action correspondant ont été regroupés en huit piliers :

- protection des infrastructures critiques et renforcement de la résilience ;
- renforcement des capacités nationales ;
- création d'un réseau organique de cybersécurité ;
- garantie de la sûreté d'utilisation des technologies de nouvelle génération ;
- lutte contre la cybercriminalité ;
- développement et diffusion des technologies nationales et locales ;
- intégration des questions de cybersécurité dans les dispositifs de sécurité nationale ;
- renforcement de la coopération internationale.

3.1 Système de suivi de la mise en œuvre des stratégies et plans d'action

Un système a été mis en place pour gérer et surveiller efficacement la mise en œuvre des stratégies et des plans d'action préparés par la présidence, ainsi que les activités du Groupe turc de la cybersécurité rattaché au Bureau de la transformation numérique. Ce dispositif contrôle le déroulement des activités et en évalue la performance et les résultats à l'aune d'objectifs prédéterminés.

Par ailleurs, le Bureau de la transformation numérique est chargé d'apporter son concours au Conseil des politiques de la science, de la technologie et de l'innovation (qui coordonne l'élaboration de politiques), notamment en ce qui concerne :

---

[79] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf.
[80] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf.
[81] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf.
[82] https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/national-cyber-security-strategy-2020-2023.pdf.

- les propositions de politiques nationales relatives à la cybersécurité et aux technologies liées aux infrastructures de communication ;
- les propositions de politiques nationales relatives aux technologies de communication de nouvelle génération (5G et technologies ultérieures) ;
- le plan d'étapes national relatif aux technologies de cybersécurité.

3.2 Mesures prises dans le cadre du programme d'action présidentiel pour l'année 2023

Conformément à la stratégie nationale de cybersécurité pour la période 2020-2023 et au plan d'action correspondant, les mesures du programme d'action présidentiel pour l'année 2023[83] qui concernent directement ou indirectement le Bureau de la transformation numérique sont les suivantes :

- actualisation de la stratégie nationale de cybersécurité, renforcement de la réglementation et de l'infrastructure technique en matière de cybersécurité et mise en place d'une structure de coordination solide :
  - élaboration d'une loi-cadre sur la cybersécurité ;
  - élaboration d'une stratégie nationale de cybersécurité pour la période 2024-2027 et d'un plan d'action connexe ;
- définition et mise en pratique des procédures et des principes régissant la mise en place de systèmes de gestion de la sécurité informatique pour les infrastructures critiques :
  - actualisation du Guide de la sécurité de l'informatique et des communications ;
- développement de produits de cybersécurité et de projets technologiques rassemblant des institutions de recherche publiques et des universités, l'objectif étant de tirer parti de l'écosystème de la cybersécurité, de créer des produits et des solutions à plus forte valeur ajoutée dans ce domaine et de les partager en code source ouvert ;
- renforcement de l'écosystème national de la cybersécurité et de sa capacité concurrentielle sur le marché mondial :
  - organisation d'un forum international des entreprises de cybersécurité ;
  - lancement d'une plateforme de diffusion des produits nationaux de cybersécurité chargée de développer un écosystème qui permettra la maturation et l'exportation des produits nationaux de cybersécurité indispensables ;
- élaboration de programmes d'études conçus pour former une main-d'œuvre qualifiée dans le domaine de la cybersécurité au sein des établissements de formation professionnelle, et définition de normes professionnelles :
  - amélioration des programmes de cybersécurité actuellement enseignés dans les établissements de formation professionnelle ;
  - définition des titres professionnels des étudiants qui seront diplômés de ces programmes et élaboration de normes à cet égard.

[83] https://www.sbb.gov.tr/wp-content/uploads/2022/11/2023-Yili-Cumhurbaskanligi-Yillik-Programi.pdf.

3.3 Mesures prises dans le cadre du programme d'action présidentiel pour l'année 2024

Conformément à la stratégie nationale de cybersécurité pour la période 2020-2023 et au plan d'action correspondant, les mesures du programme d'action présidentiel pour l'année 2024[84] qui concernent directement ou indirectement le Bureau de la transformation numérique sont les suivantes :

- renforcement de la cyberrésilience et du niveau de maturité en matière de sécurité dans l'intention de faire face aux cybermenaces qui pèsent sur les marchés financiers :
  - adoption d'un règlement visant à assurer la cybersécurité nationale et à renforcer la cyberdissuasion pour protéger le secteur financier ;
- soutien à l'harmonisation avec les normes internationales dans le domaine de la cybersécurité et à la participation de la Türkiye à des projets internationaux :
  - achèvement du règlement sur la sécurité de l'Internet des objets, en veillant à ce qu'il soit aligné sur les normes internationales et la législation de l'Union européenne (UE) ;
- adoption de règlements visant à garantir la cybersécurité nationale, en veillant à ce qu'ils soient alignés sur la directive révisée de l'UE sur la sécurité des réseaux et des systèmes d'information (SRI 2), sur les dernières initiatives de l'UE dans le domaine de la cybersécurité et sur les meilleures pratiques internationales :
  - adoption d'un règlement visant à assurer la cybersécurité nationale et à renforcer la cyberdissuasion ;
  - réalisation d'études sur la sûreté d'utilisation de l'Internet des objets en vue de réglementer ce secteur ;
  - soumission des objets connectés à des inspections de cybersécurité ;
  - définition des règlements à mettre en place pour accompagner la législation-cadre nationale sur la cybersécurité, qui fait actuellement l'objet de travaux préparatoires ;
  - organisation de travaux relatifs à la loi n° 5070 sur la signature électronique et aux textes législatifs connexes, l'objectif étant de donner une base juridique au service de signature à distance ;
  - organisation d'activités de sensibilisation visant à étendre l'utilisation du service de signature à distance dans les institutions publiques et le secteur privé ;
- coordination au plus haut niveau des activités nationales de cybersécurité et mise en place d'une structure de coordination et d'administration à même de favoriser la coopération interinstitutionnelle :
  - adoption d'une loi exclusive sur la cybersécurité régissant les fonctions, les devoirs et les responsabilités de l'organisation nationale de cybersécurité ;
  - coordination des travaux préparatoires en vue de l'élaboration de la stratégie nationale de cybersécurité pour la période 2024-2028 et du plan d'action

[84] https://www.sbb.gov.tr/wp-content/uploads/2023/10/2024-Yili-Cumhurbaskanligi-Yillik-Programi.pdf.

connexe, et mise en place d'un mécanisme de contrôle des actions et des activités dans le cyberespace ;

– organisation de travaux visant à établir un plan national de gestion des crises et des urgences en matière de cybersécurité ;

– renforcement du réseau d'échange de renseignements sur les cybermenaces ;

• renforcement des processus d'acquisition et de partage de renseignements sur les cybermenaces grâce à la diversification des sources et au développement d'applications d'intelligence artificielle et d'applications d'analyse de mégadonnées, et mise en place de mesures de détection précoce et de prévention des menaces pour la cybersécurité nationale :

– réalisation d'une analyse des besoins en sources de renseignements sur les cybermenaces ;

– renforcement de la capacité de réaction et de coordination en cas d'incident ;

– lancement de travaux concernant des projets de cybersécurité s'appuyant sur l'intelligence artificielle et l'analyse des mégadonnées, l'objectif étant de parvenir à détecter les sites Web conçus à des fins d'hameçonnage, les centres de commande et de contrôle de logiciels malveillants et les réseaux de zombies ;

• définition et mise en pratique des procédures et des principes régissant l'installation de systèmes de gestion de la sécurité informatique pour les infrastructures critiques :

– réalisation d'une analyse des processus en vue de la mise en place d'un système de gestion de la sécurité de l'information pour les infrastructures critiques ;

– organisation de travaux réglementaires en vue de l'instauration d'un système de gestion de la sécurité de l'information pour les infrastructures critiques ;

• établissement de normes de cybersécurité dans les domaines critiques :

– examen du cadre de certification établi au titre de la loi de l'UE sur la cybersécurité et définition des normes nécessaires pour les produits, services et processus de cybersécurité ;

– intégration dans le Guide de la sécurité de l'informatique et des communications d'articles relatifs aux lignes directrices du secteur privé en la matière ;

– établissement d'un modèle à utiliser pour recenser les entreprises critiques devant faire l'objet d'un contrôle conformément aux dispositions du Guide de la sécurité de l'informatique et des communications ;

– organisation des préparatifs visant à faire en sorte que les procédures de contrôle puissent être menées conformément aux dispositions du Guide de la sécurité de l'informatique et des communications ;

– organisation d'activités visant à mieux faire connaître le Guide de la sécurité de l'informatique et des communications ;

• mise en place d'infrastructures permettant de réaliser des essais relatifs à la cybersécurité :

– réalisation d'une analyse de l'ensemble actuel de centres d'application et de recherche en cybersécurité, de bancs d'essai en cybersécurité et de laboratoires de simulation des universités ;

- augmentation de l'utilisation de produits nationaux de cybersécurité, en particulier par les institutions publiques :
  - élaboration d'un plan de progression relatif au développement du secteur de la cybersécurité et à sa participation au marché mondial ;
- élaboration de programmes conçus pour former une main-d'œuvre qualifiée et améliorer les possibilités d'emploi dans le domaine de la cybersécurité :
  - organisation de concours de cybersécurité à l'intention des jeunes employés qualifiés ;
  - organisation d'activités de coopération et de coordination en vue de définir des normes professionnelles relatives aux employés du domaine de la cybersécurité ;
- amélioration du contenu et de la qualité des formations, ainsi que de l'environnement de formation, l'objectif étant de former le personnel en fonction des besoins du secteur de la cybersécurité :
  - organisation de formations à la cybersécurité en ligne et en laboratoire ;
  - poursuite des formations en ligne sur la cybersécurité données par l'Académie de l'Autorité des technologies de l'information et des communications ;
  - organisation de formations pratiques à la cybersécurité sur la plateforme de formation cyber FETIH ;
- réalisation d'études visant à sensibiliser le public à la cybersécurité :
  - réalisation d'études visant à enrichir le contenu des cours sur la cybersécurité donnés dans l'enseignement primaire et secondaire ;
  - développement de la procédure de mise en conformité et de contrôle et du programme de formation sur la sensibilisation à la sécurité de l'information prévus dans le Guide de la sécurité de l'informatique et des communications ;
  - organisation d'activités de sensibilisation aux questions de cybersécurité, telles que des séminaires, des formations et des concours ;
- renforcement des mécanismes de mise en œuvre des mesures de sécurité de l'informatique et des communications, ainsi que des mécanismes de mise en place, d'exploitation et de contrôle des systèmes de gestion de la sécurité informatique dans les institutions publiques :
  - élaboration de règlements régissant les procédures et les principes à appliquer pour garantir la sécurité de l'informatique et des communications ;
  - réalisation d'études sur les lois et les infrastructures afin de surveiller l'utilisation des noms de domaine appartenant aux institutions et organisations publiques.

4. Activités et projets du Bureau de la transformation numérique concernant l'élaboration de règlements et d'orientations de cybersécurité

Le Bureau de la transformation numérique a mené un certain nombre d'activités notables visant à renforcer la résilience nationale en prenant des mesures pour protéger les secteurs public et privé contre les cybermenaces. Ces activités ont eu pour principaux objectifs l'amélioration des réglementations et des politiques en matière de cybersécurité, la mise en place de mécanismes de contrôle, la prévention

de l'enfermement propriétaire dans les secteurs critiques, la garantie d'une transformation technologique sûre et la protection des données du pays. Certaines des études en cours sont récapitulées ci-après :

- élaboration d'un projet de règlement visant à définir les procédures et les principes à appliquer pour gérer la sécurité des sites Web hébergés par les institutions et les organisations publiques et l'attribution des sous-domaines « gov.tr» ;
- élaboration d'un projet de règlement sur la sécurité de l'informatique et des communications visant à établir des exigences techniques applicables à la mise en œuvre de mesures de sécurité de l'informatique et des communications ; ce projet de règlement prévoit également des dispositions relatives à l'établissement, à la mise en œuvre, à la maintenance, au contrôle et à l'amélioration continue des systèmes de gestion de la sécurité informatique, l'objectif étant de prévenir ou d'atténuer les risques dans ce domaine ; les exigences énoncées dans ce projet de règlement sont applicables à toutes les institutions publiques ;
- élaboration d'une loi nationale sur la cybersécurité ; cette loi a pour objectif d'assurer la gouvernance et l'organisation de la cybersécurité au niveau national au moyen d'un cadre unique de gouvernance de la cybersécurité qui soit compatible avec les évolutions technologiques et de nature à renforcer la résilience nationale face aux cybermenaces actuelles.

On trouvera dans le reste de la présente section un résumé des initiatives qui ont été mises en œuvre ou achevées.

4.1 Circulaire présidentielle 2019/12 sur les mesures de sécurité de l'informatique

La numérisation croissante de l'information, l'accès facile et direct à l'information, la numérisation des infrastructures et la prolifération des systèmes de gestion de l'information entraînent de sérieux risques pour la sécurité. Dans ce contexte, la circulaire présidentielle 2019/12 sur les mesures de sécurité de l'informatique[85] a été publiée afin de réduire les risques de sécurité rencontrés et de garantir la sécurité des données critiques dont la compromission serait susceptible de menacer la sécurité nationale ou de perturber l'ordre public. La circulaire prévoit 21 mesures de base en matière de sécurité de l'informatique et des communications[86] qui devraient être suivies par les institutions publiques et les entreprises privées offrant des services d'infrastructures critiques. Pour garantir la protection des données, la circulaire présidentielle vise à s'assurer que les données détenues par un pays restent à l'intérieur des frontières de ce pays. En outre, elle souligne que la production et l'utilisation de solutions nationales de cybersécurité constituent l'une des principales priorités de la Türkiye. Enfin, elle précise également que le Bureau de la transformation numérique sera chargé de coordonner l'élaboration du Guide de la sécurité de l'informatique et des communications dans l'intention d'atténuer et de neutraliser les risques de sécurité et surtout d'assurer la sécurité des données critiques.

4.2 Guide de la sécurité de l'informatique et des communications

Conformément à la circulaire présidentielle 2019/12 sur les mesures de sécurité de l'informatique susmentionnée, le Guide de la sécurité de l'informatique et des communications a été publié en 2020[87]. L'objectif principal de ce guide est de définir des mesures de cybersécurité détaillées à même d'assurer la sécurité des informations,

[85] https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf.
[86] cbddo.gov.tr/en/presidential-circular-no-2019-12-on-information-security-measures.
[87] cbddo.gov.tr/en/icsguide/.

des données et infrastructures critiques dont la compromission serait susceptible de perturber l'ordre public ou de menacer la sécurité nationale. Premier document de référence national publié dans ce domaine, ce guide souligne la nécessité de mettre en place une stratégie de sécurité globale portant sur tous les aspects de la sécurité de l'informatique et des communications. Il joue un rôle éminent dans le renforcement des capacités de cyberdéfense des institutions publiques et des fournisseurs de services relatifs aux infrastructures critiques. En outre, la circulaire présidentielle 2019/12 sur les mesures de sécurité de l'informatique et le Guide de la sécurité de l'informatique et des communications exigent des vendeurs de produits qu'ils fournissent une déclaration attestant que leurs produits sont exempts de portes dérobées.

4.3 Guide du contrôle de la sécurité de l'informatique et des communications

Ayant à cœur d'atteindre et de pérenniser les objectifs définis dans le Guide de la sécurité de l'informatique et des communications, et conscient du fait que la sécurité de l'informatique et des communications ne peut être assurée sans activités de contrôle et de surveillance efficaces, le Bureau de la transformation numérique a élaboré le Guide du contrôle de la sécurité de l'informatique et des communications[88] et l'a publié en octobre 2021.

Les institutions et organisations publiques et les entreprises fournissant des services d'infrastructure critiques sont tenues d'avoir achevé leurs activités de mise en conformité dans les délais indiqués dans le Guide de la sécurité de l'informatique et des communications, et de réaliser un contrôle au moins une fois par an afin de s'assurer de la conformité de leurs activités et des mesures prises.

Les organisations concernées sont non seulement tenues de se conformer aux exigences du Guide de la sécurité de l'informatique et des communications, mais aussi de procéder régulièrement à des contrôles et à des évaluations de l'efficacité de la mise en œuvre des mesures de sécurité et de la conformité du processus de mise en œuvre avec les exigences applicables. Par conséquent, des contrôles doivent être effectués au moins une fois par an par un service interne ou par une société tierce accréditée. Les politiques et procédures de contrôle à mettre en œuvre par les organisations concernées sont exposées dans le Guide du contrôle de la sécurité de l'informatique et des communications.

4.4 Programme de certification des professionnels et des entreprises chargés de contrôler la sécurité de l'informatique et des communications

Le programme de certification des professionnels et des entreprises chargés d'effectuer les contrôles de la sécurité de l'informatique et des communications conformément aux dispositions prévues dans le Guide a été conçu pour leur fournir les compétences dont ils ont besoin pour obtenir cette qualification. Le programme est mis en œuvre en coopération avec l'Institut turc de normalisation et le Conseil de la recherche scientifique et technique turc. Au total, 163 contrôleurs et 23 entreprises ont été habilités dans le cadre du programme depuis 2021.

4.5 Système de mise en conformité et de contrôle de la sécurité de l'informatique et des communications

Le système de mise en conformité et de contrôle de la sécurité de l'informatique et des communications[89] a été développé puis mis en service le 4 janvier 2023. Il permet de suivre les résultats des contrôles de toutes les organisations concernées par

[88] cbddo.gov.tr/en/icsaguide/.
[89] cbddo.gov.tr/en/bigdes/.

le Guide de la sécurité de l'informatique et des communications. Depuis le lancement du système, 2 945 utilisateurs et 1 191 organisations se sont déjà inscrits. Les organisations peuvent fournir des informations sur l'état d'avancement des activités de mise en conformité et de contrôle qu'elles mènent conformément au Guide de la sécurité de l'informatique et des communications. Cette plateforme numérique permet également de surveiller le niveau de conformité actuel des systèmes de gestion de la sécurité informatique des organisations.

4.6 Projet d'analyse et de rapport sur le modèle national de gouvernance de la cybersécurité

Le projet d'analyse et de rapport sur le modèle national de gouvernance de la cybersécurité, lancé pour examiner le modèle de gouvernance de la cybersécurité en Türkiye, a été achevé. Une analyse comparative de différents pays a été réalisée, et des pistes d'amélioration recommandées. Un cadre de gouvernance de la cybersécurité a été élaboré pour la Türkiye sur cette base.

Après l'achèvement du projet, un atelier national sur la cybersécurité a été organisé le 13 décembre 2022 afin de partager les résultats du projet, au cours duquel plus de 40 institutions publiques et 100 participants ont donné leurs avis et formulé des suggestions. Les conclusions de l'atelier ont fait apparaître qu'il était nécessaire d'adopter une loi nationale sur la cybersécurité. Cette loi est en cours d'élaboration.

5. Activités et projets du Bureau de la transformation numérique concernant l'écosystème de la cybersécurité

5.1 Groupe turc de la cybersécurité

En octobre 2017, les institutions du secteur public, les universités et les principales entreprises de cybersécurité du secteur privé ont été invitées à discuter des possibilités de coopération entre elles, donnant ainsi naissance au Groupe turc de la cybersécurité[90]. Aujourd'hui, le Groupe opère sous la coordination du Bureau de la transformation numérique et du Secrétariat des entreprises du secteur de la défense et rassemble plus de 200 membres qui proposent plus de 400 produits et services. Le Groupe turc de la cybersécurité est également membre du réseau Global EPIC (Global Ecosystems Partnered in Innovation and Cybersecurity) depuis 2018.

Parmi les objectifs du Groupe turc de la cybersécurité, citons :

- l'augmentation du nombre d'entreprises de cybersécurité ;
- la fourniture d'un soutien au développement des capacités techniques, administratives et financières des entreprises membres ;
- l'amélioration de l'image de marque des produits et des services ;
- l'enrichissement des normes de l'écosystème de la cybersécurité ;
- le renforcement de la capacité concurrentielle des entreprises membres sur les marchés nationaux et mondiaux ;
- le développement du capital humain dans le domaine de la cybersécurité ;
- la progression de la sensibilisation du grand public aux questions de cybersécurité.

Bien qu'il n'y ait pas d'obligation légale pour les entreprises privées de participer à cette coopération, l'accent est mis sur la confiance mutuelle et la collaboration entre le secteur public et les institutions privées. La raison d'être de

[90] https://siberkume.org.tr/.

cette initiative est de renforcer les relations acheteur-fournisseur, les circuits de distribution communs, les possibilités de mise en réseau et les activités de recherche et de développement menées par les universités avec les entreprises, qui peuvent créer de meilleurs débouchés et de meilleurs avantages pour les deux parties. En raison de leurs intérêts économiques communs, les entreprises du Groupe sont devenues plus productives, plus innovantes et donc plus compétitives que les entreprises opérant seules.

Il n'est généralement pas possible de réussir dans le domaine de la cybersécurité sans le soutien de l'autorité publique au plus haut niveau. Certaines entreprises turques se sont développées à l'étranger et y commercialisent des produits de cybersécurité homologués et uniques qui figurent parfois dans les rapports de l'entreprise de conseil Gartner, comme c'est le cas de certains logiciels de simulation d'intrusion et d'attaque.

5.2 Conseil des relations économiques extérieures – Conseil sectoriel des technologies numériques (DIGITECH) – Comité de la cybersécurité

Soucieuse d'accroître l'efficacité de ses entreprises nationales à l'étranger, la Türkiye a lancé son Conseil sectoriel des technologies numériques (DIGITECH)[91] en juin 2022 avec le soutien du Bureau de la transformation numérique et sous la coordination du Conseil des relations économiques extérieures. DIGITECH s'est engagé à mener des projets sur les sujets suivants :

- la mondialisation de l'écosystème des technologies numériques de la Türkiye ;
- l'adaptation aux nouvelles tendances ;
- l'accès aux financements internationaux, la transformation numérique et la réglementation du secteur.

Les objectifs de DIGITECH sont les suivants :

- augmenter le nombre d'entreprises turques figurant au classement Fortune 500 et le nombre de licornes turques ;
- faire de la Türkiye un pôle technologique et créer des couloirs numériques avec d'autres pays ;
- renforcer les exportations turques de produits de pointe ;
- promouvoir l'internationalisation des entreprises du secteur par l'intermédiaire des 144 bureaux commerciaux bilatéraux du Conseil des relations économiques extérieures ;
- soutenir la transformation numérique des groupes industriels en les associant à des start-ups ;
- augmenter le capital-innovation dans le secteur, tant en taille qu'en nombre, en créant des plateformes destinées à rassembler le capital-innovation mondial, le capital-innovation national, les scale-ups et les start-ups ;
- recenser les problèmes rencontrés par les entreprises du secteur et informer les organes publics compétents de ces problèmes.

Les sous-comités de DIGITECH sont consacrés aux secteurs suivants : informatique en nuage, technologie financière, technologie mobile, jeux, cybersécurité, logiciels, technologies innovantes, capital-innovation, technologies de la santé, Web3-chaîne de blocs. Comme on peut le voir, DIGITECH est organisé selon

[91] www.deik.org.tr/sectoral-business-councils-digital-technologies-business-council?pm=65.

une structure sectorielle et dispose d'un sous-comité spécialisé dans les questions de cybersécurité.

La Türkiye considère le développement de technologies nationales de cybersécurité comme un enjeu stratégique et une question de sécurité nationale. En conséquence, elle met l'accent sur la création de produits et de services robustes et à grande échelle, capables de rivaliser avec leurs équivalents étrangers. Le marché mondial de la cybersécurité connaît depuis peu une croissance importante, alimentée par la prise de conscience des risques et des menaces qui pèsent sur les données. Le marché des produits et services de cybersécurité devrait continuer à croître.

La Türkiye est présente sur ce marché en expansion et collabore avec le secteur privé et les institutions gouvernementales pour développer ses solutions à l'échelle mondiale. Le Bureau de la transformation numérique met par conséquent tout en œuvre pour renforcer les technologies nationales de cybersécurité, conformément au mandat qui lui a été confié dans le décret présidentiel n° 1, en vertu duquel il a notamment été chargé de réaliser des études visant à développer des produits nationaux de cybersécurité dans tous les secteurs, en particulier les secteurs liés aux infrastructures critiques, et de promouvoir leur utilisation dans le secteur public.

Soucieuse de stimuler la croissance de l'écosystème national de la cybersécurité, la Türkiye a adopté une approche systématique en coordination avec le Bureau de la transformation numérique, l'objectif étant d'intégrer le système d'incitation aux procédures de passation des marchés publics, d'évaluer les niveaux de maturité des produits nationaux de cybersécurité et de les améliorer et les développer progressivement.

Le Groupe de coordination nationale en matière de cybersécurité a été créé en 2021 en coordination avec le Bureau de transformation numérique et sous la direction du Secrétariat des entreprises du secteur de la défense, du Ministère de l'industrie et de la technologie, du Service national des approvisionnements, de l'Agence des marchés publics et de la présidence de la stratégie et du budget. Le Ministère du Trésor et des finances, le Conseil de la recherche scientifique et technique turc, l'Institut turc de normalisation, TURKSAT, le Ministère des transports et des infrastructures et l'Autorité des technologies de l'information et des communications ont ensuite rejoint le Groupe, dont l'objectif principal est d'encourager l'utilisation de produits de cybersécurité nationaux dans tous les secteurs, tant au niveau national qu'international, en mettant l'accent sur le secteur public. Les activités du groupe sont divisées en cinq piliers principaux : politiques, législation, normalisation/maturité, incitations/aides/financements et internationalisation.

6. Activités et projets du Bureau de la transformation numérique concernant la sensibilisation aux questions de cybersécurité

6.1 Concours de cybersécurité organisés dans le cadre du festival TeknoFest

Le Bureau de la transformation numérique est conscient du fait que le besoin de connaissances et de compétences en matière de cybersécurité devient de plus en plus urgent du fait de l'importance accordée aux technologies de l'information et des communications. Dans cette perspective, il s'emploie également à organiser des concours visant à sensibiliser le public aux questions de cybersécurité, dont l'un des exemples les plus remarquables est « HackIstanbul ». Reconnu dans le monde entier comme un concours extraordinaire, « HackIstanbul » est organisé depuis 2018 dans le cadre du festival de l'aviation, de l'espace et de la technologie TeknoFest[92]. Ces concours ont ouvert leurs portes à tous les hackers du monde entier pour qu'ils

[92] www.teknofest.org/en/.

puissent montrer leurs talents. Si les concours tenus à Istanbul portaient le nom de « HackIstanbul », l'édition exceptionnelle organisée en 2020 à Gaziantep était quant à elle intitulée « HackZeugma ». En août 2022, le Bureau de la transformation numérique a organisé le concours « HackBlackSea 2022 » à Zonguldak.

Les candidatures pour le concours « HackMasters 2023 », qui s'est tenu le 23 avril de cette année, ont été clôturées en mars 2023. Les finalistes ont été désignés au terme d'une chasse aux primes organisée en ligne. Lors de la phase finale, qui s'est déroulée le 28 avril, les candidats ont été confrontés à un scénario axé sur les failles de sécurité des appareils intelligents. Pour l'emporter, les hackers devaient réussir à prendre le contrôle d'appareils domestiques intelligents en trouvant et en exploitant des failles de sécurité dans les systèmes eux-mêmes, dans les applications mobiles qu'ils contiennent et dans les infrastructures en nuage avec lesquelles ils échangent des données.

Les concepts abordés dans le cadre du concours varient d'une année à l'autre et vont de la sécurité des systèmes technologiques opérationnels à des défis de type « primes aux bogues » ou « capture du drapeau ». Si ces concours ont avant tout pour objectif de sensibiliser le public aux questions de cybersécurité et d'attirer de nouveaux talents dans le secteur, ils offrent par ailleurs une vitrine mondiale au secteur turc de la cybersécurité.

La date limite de dépôt des candidatures pour le concours « HackMasters 2024 »[93] est fixée au 31 mai 2024, et la phase finale se tiendra en août 2024 à Istanbul dans le cadre du TeknoFest[94].

6.2 Concours de cyberrenseignement

Le Bureau de la transformation numérique organise également plusieurs camps et programmes de formation en matière de cybersécurité, ainsi que des exercices de type « capture du drapeau » avec des acteurs issus d'institutions publiques cibles, telles que le Ministère de l'éducation nationale et le Ministère de la jeunesse et des sports, du secteur privé et d'organisations non gouvernementales. Ces camps et programmes de formation permettent de faire en sorte que suffisamment de jeunes décident de mettre à profit leur talent dans le secteur de la cybersécurité. Il est également à noter que plus d'un million d'étudiants participent à ces événements.

Parmi les autres exemples d'événements notables, citons les concours de cyberrenseignement[95] organisés dans le cadre d'activités de formation et de sensibilisation visant à accroître le nombre de personnes ayant des notions de cybersécurité, mission pour laquelle ils se sont avérés d'une grande efficacité. Au total, 1,5 million d'élèves ont participé à ces concours, qui se déroulent en ligne et sont organisés séparément pour les niveaux d'enseignement élémentaire, secondaire inférieur et secondaire supérieur. Les questions sont préparées par le Bureau de la transformation numérique et parachevées avec le soutien du Ministère de l'éducation nationale en tenant compte du programme scolaire en vigueur, et les annonces sont faites sur les comptes du Bureau de la transformation numérique, du Ministère de l'éducation nationale et de la plateforme EBA (réseau d'information sur l'éducation) sur les réseaux sociaux. Dans le cadre de ces concours, les élèves qui donnent le plus de réponses correctes dans le temps le plus court possible reçoivent des cadeaux et des récompenses surprises afin de stimuler leur intérêt pour ce domaine.

La quatrième édition du concours de connaissances en matière de cyberrenseignement a eu lieu en 2023. Organisé pour la première fois en octobre 2020

[93] https://hackmasters.com.tr/.
[94] www.teknofest.org/en/competitions/hack-masters/.
[95] https://cbddo.gov.tr/en/projects/cyberintelligencecontest/.

en collaboration avec la présidence et le Ministère de l'éducation nationale, ce concours s'adresse aux élèves des niveaux d'enseignement élémentaire, secondaire inférieur et secondaire supérieur. Il a eu lieu le 27 décembre 2023 pour les élèves de l'enseignement élémentaire (16 915 inscrits), le 28 décembre 2023 pour les élèves de l'enseignement secondaire inférieur (15 955 inscrits) et le 29 décembre 2023 pour les élèves de l'enseignement secondaire supérieur (4 528 inscrits).

6.3 Dessin animé abordant des sujets liés au numérique

Après avoir mené de nombreuses études sur la sensibilisation aux questions de cybersécurité à l'échelle nationale, le Bureau de la transformation numérique estime également qu'il faut améliorer l'habileté numérique des enfants même lorsque ces derniers ne sont pas en ligne. Loin de se limiter à un savoir-faire technique, le concept d'habileté numérique désigne l'ensemble des connaissances, des compétences et des attitudes qui permettent aux enfants d'être à la fois en sécurité et autonomes dans le monde numérique. L'un des principaux projets développés à cette fin à l'intention des enfants est une série de dessins animés appelée *Digital Crew*[96]. Diffusée sur la chaîne de radio et de télévision destinée à la jeunesse Çocuk depuis 2020, cette série a pour objectif principal d'améliorer les connaissances, l'habileté et la conscience numériques des enfants. Le contenu de *Digital Crew* a été préparé en coopération avec le Bureau de la transformation numérique et comprend 10 épisodes qui abordent un large éventail de sujets allant de la sécurité des enfants sur Internet au harcèlement en ligne, en passant par la dépendance à Internet, l'intelligence artificielle, l'Internet des objets, les effets de la numérisation sur le quotidien et les technologies nationales.

7. Activités et projets du Bureau de la transformation numérique concernant l'éducation à la cybersécurité

La disponibilité de ressources humaines dotées de compétences et de connaissances adéquates constitue à n'en pas douter l'un des facteurs les plus importants pour garantir la cybersécurité nationale. Afin de répondre aux besoins de notre pays dans ce domaine, le Bureau de la transformation numérique mène des activités visant à accroître le niveau de compétence des ressources humaines existantes. Certaines de ces initiatives sont détaillées ci-après.

7.1 Mise en place d'un lycée de formation professionnelle en cybersécurité en coopération avec le Ministère de l'éducation nationale de la République de Türkiye

Des mesures concrètes ont été prises pour développer les compétences et les capacités de cybersécurité dans l'enseignement formel et ont mené au lancement du programme d'études élaboré à cet effet pour l'enseignement secondaire en 2020.

Premier lycée de Türkiye à proposer une formation en cybersécurité, le lycée de formation professionnelle et technique Teknopark Istanbul a été créé par le Ministère de l'éducation nationale avec la contribution du Groupe turc de la cybersécurité, du Secrétariat des entreprises du secteur de la défense, du Bureau de la transformation numérique et de Teknopark Istanbul. Située sur le campus de Teknopark Istanbul, l'école propose des programmes axés sur les technologies de l'information, la gestion des réseaux et la cybersécurité.

Le lycée de formation professionnelle en cybersécurité est en tête de liste des préférences depuis le jour de son ouverture.

---

[96] www.youtube.com/watch?v=YnuLs6GAogM&ab_channel=CBDijitalD%C3%B6n%C3%BC%C5%9F%C3%BCmOfisi .

7.2 Mise en place d'établissements de formation professionnelle en cybersécurité en coopération avec le Conseil de l'enseignement supérieur de la République de Türkiye

Le Bureau de la transformation numérique a lancé un nouveau projet visant à former du personnel qualifié dans le domaine de la cybersécurité en poussant plus loin le modèle appliqué dans le lycée de formation professionnelle en cybersécurité susmentionné. La première étape vers l'ouverture d'établissements de formation professionnelle en cybersécurité a été franchie en 2022 avec la signature d'un protocole de coopération entre le Bureau de la transformation numérique et le Conseil de l'enseignement supérieur[97].

Ces établissements, qui proposent des programmes d'enseignement uniquement dans le domaine de la cybersécurité, ont été ouverts en 2023. Le premier programme qui y est proposé forme des analystes et des opérateurs en cybersécurité[98]. Ce programme a été lancé dans quatre des principales universités de Türkiye, à savoir l'université d'Ankara, l'université de l'Égée, l'université technique de Gebze et l'université technique d'Istanbul.

8. Place de la Türkiye dans les classements mondiaux des pays les plus avancés en matière cybersécurité

L'adoption des technologies numériques au niveau local et national a poussé la Türkiye à placer sur un pied d'égalité la cybersécurité et la sécurité physique du pays. Face à la montée de la menace cyber, des investissements adéquats ont été réalisés dans les secteurs public et privé de la cybersécurité. De nombreux projets coordonnés ont été menés dans les domaines public, privé et militaire ; d'importants investissements ont été réalisés par de grandes organisations du secteur de la défense ; des instituts spécialisés dans la cybersécurité ont été créés dans le domaine universitaire ; de nouveaux produits et technologies ont été développés grâce aux capacités nationales. La Türkiye est ainsi devenue depuis peu l'un des pays les plus performants dans le domaine de la cybersécurité.

L'action menée par le Gouvernement et les acteurs du secteur public pour atteindre ces objectifs a permis à la Türkiye de gagner des places dans les classements mondiaux des pays les plus avancés en matière de cybersécurité.

La Türkiye figure parmi les pays dont l'indice de cybersécurité est le plus élevé au monde, ce qui témoigne des résultats obtenus par le pays jusqu'à présent.

Selon l'indice mondial de cybersécurité publié par l'Union internationale des télécommunications (UIT) en 2021[99], la Türkiye occupe la onzième place au classement mondial, soit une progression de neuf places par rapport à l'année précédente, et la sixième place au classement européen.

Les technologies de l'information et des communications jouent un rôle indispensable dans le monde actuel. Elles sont le système nerveux de nos sociétés qui relie de manière complexe les économies, les gouvernements et les individus aux quatre coins du globe. Imaginer un monde sans communication instantanée, sans accès permanent à l'information ou sans la possibilité de faire des affaires par voie électronique, c'est imaginer une réalité fondamentalement différente. Les technologies de l'information et des communications ont eu une incidence manifeste sur toutes les facettes de la vie humaine, de la diffusion des connaissances à la fourniture de soins de santé, en passant par le divertissement et les interactions

---

[97] cbddo.gov.tr/projeler/siber-myo/.

[98] cbddo.gov.tr/sss/siber-myo/.

[99] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-F.pdf.

sociales. Elles permettent aux citoyens de s'émanciper, favorisent les percées novatrices et stimulent la croissance économique à un rythme sans précédent. En outre, les pouvoirs publics peuvent exploiter la puissance des technologies de l'information et des communications pour fournir des services plus efficaces, plus transparents et plus inclusifs, favorisant ainsi un cadre démocratique plus participatif et plus solide.

Toutefois, si ce paradigme de connectivité offre d'immenses avantages, il s'accompagne également d'une importante réserve : la sécurité. Notre dépendance à l'égard des technologies de l'information et des communications s'accroît sans cesse, tout comme notre vulnérabilité face aux cybermenaces. Les acteurs malveillants, qu'il s'agisse de cybercriminels cherchant à s'enrichir personnellement ou d'entités parrainées par des États poursuivant des objectifs géopolitiques, exploitent ces failles pour cibler les infrastructures critiques, les systèmes publics stockant des données sensibles et les données personnelles des citoyens. L'interconnexion mondiale des infrastructures informatiques crée un réseau complexe d'interdépendances, où une seule faille de sécurité dans un coin reculé du monde peut avoir des effets en cascade ailleurs, risquant ainsi de perturber des services essentiels, de provoquer des difficultés économiques ou de miner la confiance du public. L'émergence de nouvelles technologies, telles que l'intelligence artificielle et l'Internet des objets, introduit une toute nouvelle dimension de défis en matière de sécurité qui nécessitent une attention immédiate et le développement de solutions innovantes, car ces technologies introduisent souvent de nouveaux vecteurs d'attaque et des complexités propres à la sécurisation de vastes réseaux d'appareils interconnectés.

Il est donc impératif d'emprunter une voie qui favorise un équilibre judicieux entre l'exploitation de l'immense potentiel des technologies de l'information et des communications et l'atténuation des risques qui y sont associés. Les États doivent avant tout garantir la sûreté d'utilisation des technologies de l'information et des communications et faire de cette question un enjeu de sécurité nationale. Il faut à cette fin adopter une approche à plusieurs composantes. Il est primordial d'élaborer des stratégies nationales solides en matière de cybersécurité, soutenues par des partenariats public-privé robustes qui tirent parti des compétences spécialisées et des ressources des pouvoirs publics et du secteur privé.

Les initiatives menées conjointement par les pouvoirs publics et les entreprises pour investir dans des activités de formation et de sensibilisation des citoyens et des fonctionnaires aux questions de cybersécurité sont tout aussi essentielles. Ces formations devraient non seulement porter sur les compétences techniques nécessaires pour détecter et atténuer les cybermenaces, mais aussi sur la promotion d'une culture de la cyberhygiène auprès des citoyens.

En outre, la promotion de la coopération internationale en matière de sécurité des technologies de l'information et des communications reste indéniablement essentielle. Sur ce point, la poursuite d'un dialogue institutionnel régulier sous l'égide de l'ONU est très importante. Les États Membres doivent travailler ensemble à la création d'un cadre de normes internationales et de cadres juridiques favorisant un comportement responsable des États dans le cyberespace. Ce cadre devrait prévoir des protocoles d'échange d'informations susceptibles de faciliter la réaction rapide aux cybermenaces, des efforts de coopération en matière d'application de la loi et de lutte contre la cybercriminalité et l'élaboration de traités internationaux établissant des normes de comportement acceptable dans le cyberespace. En fin de compte, l'objectif va au-delà des mesures purement défensives visant à construire des infrastructures informatiques résilientes et consiste notamment à concevoir des systèmes qui ont non seulement la force de résister aux cyberattaques, mais aussi la capacité de se rétablir rapidement, de minimiser les perturbations et de maintenir

l'intégrité des données. En outre, il est important de promouvoir le développement et l'utilisation éthiques des technologies de l'information et des communications. Les États Membres peuvent faire en sorte que cette puissante technologie soit mise au service de valeurs d'humanisme en donnant la priorité à la protection de la vie privée des utilisateurs, en préconisant des pratiques de recherche responsables qui réduisent au minimum les risques d'utilisation abusive et en garantissant la transparence dans le développement et le déploiement des systèmes informatiques.

En donnant la priorité à la sécurité tout en promouvant l'innovation, les États Membres peuvent faire en sorte que les technologies de l'information et des communications continuent à jouer un rôle transformateur et positif dans l'évolution de notre monde. Cette approche collaborative, associée à une vigilance et à une adaptation permanentes, est essentielle pour assurer un avenir numérique sûr et prospère pour tous.

Venezuela (République bolivarienne du)

[Original : espagnol
26 avril 2024]

Au paragraphe 8 de sa résolution 78/237 adoptée le 22 décembre 2023, l'Assemblée générale invite tous les États Membres à continuer d'informer le Secrétaire général de leurs vues et évaluations sur la sécurité du numérique et de son utilisation, en particulier sur le futur dialogue institutionnel régulier relatif à ces questions sous les auspices de l'Organisation des Nations Unies, et prie le Secrétaire général de lui présenter un rapport fondé sur ces vues durant sa soixante-dix-huitième session, afin que les États Membres puissent en débattre plus avant lors des réunions du Groupe de travail à composition non limitée à sa huitième session, en 2024.

À cet égard, la République bolivarienne du Venezuela estime qu'il est nécessaire de souligner l'importance du groupe de travail à composition non limitée et de ses modalités de travail aux fins de l'exécution du mandat confié par l'Assemblée générale, tel qu'il est défini dans la résolution 75/240. Les réalisations de ces dernières années, telles que la création du répertoire mondial et intergouvernemental d'interlocuteurs, démontrent que le format actuel du groupe de travail à composition non limitée a été très efficace, notamment parce qu'il repose sur le consensus dans la prise de décision et dans l'adoption des rapports annuels.

La République bolivarienne du Venezuela réaffirme que l'Organisation des Nations Unies devrait continuer de jouer un rôle fondamental et central pour ce qui est de promouvoir le dialogue sur l'utilisation du numérique par les États. Le caractère particulier des technologies de l'information et des communications rend nécessaire l'élaboration de nouveaux principes et règles, de préférence juridiquement contraignants, pour combler les lacunes entre le droit international existant et les réalités d'un environnement virtuel.

À la lumière de ce qui précède, il est jugé urgent d'assurer la continuité des travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) au moyen d'un nouveau groupe de travail permanent à composition non limitée qui sera établi après 2025, ce qui contribuera à renforcer la capacité de cette nouvelle itération du groupe de travail d'élaborer et d'adapter de nouvelles normes juridiquement contraignantes qui aideront à renforcer la sécurité internationale dans l'utilisation des technologies de l'information et des communications.

Il est également urgent de doter le prochain groupe de travail à composition non limitée créé après 2025 de la capacité de relever les défis liés à l'importante fracture

numérique qui existe entre les pays membres, fossé qui rend difficile la concrétisation de stratégies globales de renforcement de la sécurité internationale dans l'utilisation du numérique.

Enfin, la République bolivarienne du Venezuela soutient pleinement les efforts considérables déployés par le Président du groupe de travail à composition non limitée pour parvenir à un consensus dans toutes les activités du groupe et réaffirme qu'elle continuera de participer à ce processus et de l'appuyer.

Réponses reçues d'organisations intergouvernementales

Union européenne

[Original : anglais
29 avril 2024]

Le cyberespace, et en particulier l'Internet mondial et ouvert, est devenu l'épine dorsale de notre société. Il offre une plateforme qui stimule la connectivité et la croissance économique. L'Union européenne et ses États membres sont favorables à un cyberespace mondial ouvert, stable et sûr, reposant sur l'état de droit, les droits humains, les libertés fondamentales et les valeurs démocratiques, un socle qui est propice au développement social, économique et politique partout dans le monde.

La communauté internationale affirme que le droit international existant, y compris la Charte des Nations Unies dans son intégralité, s'applique au comportement des États dans le cyberespace et qu'il est essentiel au maintien de la paix et de la stabilité et à la promotion d'un environnement ouvert, sûr, pacifique et accessible en matière de technologies de l'information et des communications.

Les recommandations par consensus formulées par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale en 2010, 2013, 2015 et 2021, celle du groupe de travail à composition non limitée chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale datant de 2021 et les rapports d'activité annuels de 2022 et 2023 du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), qui font également l'objet d'un consensus, ont bâti et consolidé un cadre de comportement responsable des États dans le cyberespace. Le cadre prévoit l'application du droit international au cyberespace, les normes volontaires de comportement responsable des États, ainsi que des mesures de confiance et de renforcement des capacités.

L'Union européenne et ses États membres réaffirment qu'ils sont déterminés à agir dans le respect de ces accords existants et du droit international, y compris la Charte dans son intégralité, et des normes de comportement responsable des États dans le cyberespace. Nous sommes déterminés à promouvoir et à faire progresser la paix et la stabilité dans le cyberspace grâce à des discussions et des espaces tels que l'actuel groupe de travail à composition non limitée.

Dans ce contexte, et comme suite au soutien apporté aux travaux du groupe de travail à composition non limitée, l'Union européenne n'a pas été en mesure d'appuyer la résolution 78/237, intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale », adoptée par l'Assemblée générale le 22 décembre 2023.

L'Union européenne estime que la résolution aurait pu mieux représenter le fragile consensus obtenu dans le groupe de travail à composition non limitée, les processus qui l'ont précédé et les résolutions de consensus antérieures.

Au premier chef, la résolution ne fait pas référence au cadre cumulatif et évolutif du comportement responsable des États pour ce qui est de l'utilisation du numérique, cadre qui est le fruit de plus de 20 ans de négociations et qui a été approuvé à plusieurs reprises par consensus par l'Assemblée générale.

Au contraire, elle met en évidence, notamment à l'alinéa 16 du préambule et au paragraphe 5, certaines propositions de fond soutenues par un petit groupe d'États, dont l'Union européenne craint qu'elles n'entravent l'approche progressive et consensuelle grâce à laquelle le groupe de travail à composition non limitée a pu avancer au cours de ces dernières années.

L'Union européenne et ses États membres considèrent que l'application du cadre de comportement responsable des États en matière d'utilisation des technologies de l'information et des communications est de la plus haute importance pour garantir un environnement numérique ouvert, sûr, stable, accessible et pacifique ; ils s'inquiètent de constater que cette résolution s'appuie sur un texte non consensuel qui pourrait conduire à réinterpréter les travaux du groupe de travail à composition non limitée et les documents consensuels existants.

L'Union européenne reste pleinement déterminée à trouver un terrain d'entente pour faire progresser le consensus dans l'actuel groupe de travail à composition non limitée et à déployer des efforts collectifs pour concevoir un mécanisme inclusif, permanent et pragmatique en vue d'un dialogue institutionnel régulier à l'issue des travaux de l'actuel groupe de travail à composition non limitée.

En ce qui concerne les demandes formulées au titre du paragraphe 8 de la résolution

Des progrès considérables ont été accomplis dans les débats sur un futur mécanisme après la conclusion des travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). Le rapport du Secrétaire général (A/78/76) faisant suite à la résolution 77/37 de l'Assemblée générale présentait les observations et conclusions des États Membres 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. De plus, le groupe de travail à composition non limitée est parvenu à un consensus sur des éléments communs pour un futur mécanisme de dialogue institutionnel régulier dans son rapport d'activité annuel de 2023. Enfin, le Président dudit groupe de travail à composition non limitée a proposé d'autres éléments communs dans un document de travail, en s'appuyant sur les propositions des délégations et les discussions de la sixième session de fond du groupe de travail à composition non limitée.

Compte tenu des progrès réalisés dans le recensement des éléments communs d'un futur mécanisme, l'Union européenne continuera de faire part de son point de vue sur un futur mécanisme de dialogue institutionnel régulier.

La promotion de la sécurité et de la stabilité internationales dans le cyberespace, et l'amélioration de la compréhension et de l'application du cadre de l'Organisation des Nations Unies de comportement responsable des États dans le cyberespace, devraient rester des priorités du dialogue institutionnel régulier mené sur ces questions sous les auspices de l'Organisation.

Répondant à l'appel tendant à établir un dialogue institutionnel permanent, inclusif et transparent et à large participation, sous les auspices de l'Organisation des Nations Unies, tel que décrit dans les rapports de 2021 du groupe de travail à composition non limitée chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et du Groupe d'experts gouvernementaux, le programme d'action, proposition initiée par un groupe interrégional[100], constitue une occasion de proposer une structure permanente aux fins de la tenue d'un dialogue institutionnel régulier au niveau de l'Organisation et donc de permettre à la communauté internationale d'axer ses discussions sur le fond plutôt que d'avoir des débats récurrents sur les processus à venir. Dans ce contexte, le programme pourrait devenir le mécanisme évolutif de la coopération future au sein de la Première Commission de l'Assemblée générale.

À cette fin, l'objectif collectif devrait être de trouver un équilibre entre deux aspects également importants de nos activités : l'application du cadre établi de comportement responsable des États dans l'utilisation du numérique dans le contexte de la sécurité internationale, et la poursuite du développement de ce cadre. L'élaboration du cadre découle, entre autres, des enseignements tirés de la mise en œuvre des engagements existants.

Le mécanisme devrait être inclusif et pragmatique, servir de plateforme pour des discussions et des échanges détaillés, faciliter le renforcement des capacités et permettre la poursuite du développement du cadre normatif et sa mise à jour en fonction des évolutions en cours dans l'environnement numérique, sur la base d'un consensus.

Il devrait également prévoir la participation formelle et des consultations régulières des parties prenantes concernées, y compris le secteur privé, le milieu universitaire et la société civile, afin qu'elles puissent examiner ces questions et apporter leurs points de vue et leur expertise uniques. Il sera ainsi possible de concentrer davantage les efforts déployés quant à l'aide apportée aux États en matière de promotion de l'application du cadre de comportement responsable des États et de renforcement des capacités en fonction des besoins afin d'accroître la cyberrésilience tant au niveau national que mondial.

Le programme d'action devrait être fondé sur le cadre normatif contenu dans les rapports de consensus successifs du Groupe d'experts gouvernementaux et du groupe de travail à composition non limitée, ainsi que sur les engagements et les mesures qui en découlent. Dans le cadre du futur mécanisme, on devrait convoquer des conférences d'examen périodiques à quelques années d'intervalle (par exemple, tous les trois ou quatre ans) pour revoir le cadre de comportement responsable des États, le mettre à jour si nécessaire et donner une orientation stratégique aux travaux du mécanisme.

Dans le cadre du programme d'action, on pourrait tenir des sessions formelles annuelles, qui rassembleraient les travaux détaillés et ouverts de l'année. Au cours de sessions formelles annuelles, on pourrait décider de réunions, de groupes de travail ou d'axes de travail techniques à composition non limitée, afin d'axer les travaux sur des questions prioritaires précises devant progresser dans le cadre du programme.

La participation aux groupes de travail techniques devrait être volontaire et ouverte à tous les États. Les éléments tels que la structure des axes de travail, ainsi que la participation des parties prenantes, et la fréquence des réunions, devraient être décidés lors des réunions annuelles ou des conférences d'examen. Ces réunions

[100] Voir https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf (en anglais).

devraient être orientées vers l'élaboration d'un document final présentant des conclusions opérationnelles fondées sur les enseignements tirés de l'application du cadre de comportement responsable des États, dans un cycle d'amélioration continue.

Le programme d'action pourrait aussi renforcer le dialogue régional par la coopération avec les organisations régionales, l'objectif étant de tirer parti des initiatives pertinentes existantes et de s'appuyer sur les structures et les plateformes de renforcement des capacités existantes. Ces efforts collectifs aideraient les pays à définir leurs besoins en matière de renforcement des capacités et à les satisfaire. Il incombe au premier chef aux États de maintenir la paix et la sécurité internationales et ils jouent un rôle central dans la mise en place du programme d'action ; toutefois, les échanges et la collaboration avec les parties prenantes pourraient être renforcés en offrant un espace favorisant une participation inclusive et entière.

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 devraient être organisées en 2024 et 2025 afin de poursuivre l'élaboration des différents aspects du programme d'action, y compris les implications budgétaires relatives au mécanisme permanent et le recensement des acteurs concernés dans l'Organisation qui pourraient remplir ces fonctions. Le groupe de travail à composition non limitée actuel devrait donc y consacrer des sessions, dont il ferait figurer les conclusions dans les rapports d'activité correspondants. Le programme d'action devrait être prêt à l'issue des travaux du groupe de travail à composition non limitée.