Nations Unies A/AC.292/2024/2

Assemblée générale

Distr. générale
22 janvier 2024
Français
Original : anglais

Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025)
Septième session de fond
New York, 4-8 mars 2024

État des lieux en vue d'examiner les programmes et les initiatives de renforcement des capacités qui existent actuellement au sein et en dehors du système des Nations Unies et aux niveaux mondial et régional

Document du Secrétariat

I. Introduction

1. Au paragraphe 46 du rapport sur l'état d'avancement des discussions du groupe de travail sur le point 5 de l'ordre du jour, figurant en annexe du document intitulé « Progrès de l'informatique et des télécommunications et sécurité internationale » (A/78/265), le Secrétariat de l'ONU a été prié de procéder à un « état des lieux », en consultation avec les entités concernées, afin d'examiner les programmes et les initiatives de renforcement des capacités qui existent actuellement au sein et en dehors du système des Nations Unies et aux niveaux mondial et régional, y compris en sollicitant les vues des États Membres. Le Secrétariat a en outre été prié d'établir un rapport sur les résultats de cet « état des lieux » et de le présenter à la septième session du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), qui se tiendra du 4 au 8 mars 2024, afin d'aider les États à faire le point sur les activités de renforcement des capacités en matière de sécurité numérique et d'encourager de nouvelles synergies et une meilleure coordination entre ces activités. Le présent rapport fait suite à cette demande.

2. Le 2 octobre 2023, le Bureau des affaires de désarmement a diffusé une note verbale auprès de toutes les missions permanentes auprès de l'ONU pour attirer leur attention sur le paragraphe 46 du rapport susmentionné, les invitant à donner leur avis sur les programmes et les initiatives de renforcement des capacités qui existent actuellement au sein et en dehors du système des Nations Unies et aux niveaux mondial et régional. Le délai de réponse a été fixé au 10 novembre 2023, puis prolongé jusqu'au 16 novembre. Au 22 janvier 2024, les États suivants avaient présenté des observations écrites : Allemagne, Australie, Belgique, Brésil, Burkina Faso, Cambodge, Chili, Colombie, Cuba, Estonie, France, Inde, Iran (République

islamique d'), Tchéquie, Pays-Bas (Royaume des), États-Unis d'Amérique, Fédération de Russie, Liban, Mexique, Portugal, Qatar, République de Corée, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Singapour, Slovaquie, Slovénie, Suisse, Türkiye et Uruguay.

3. Le Bureau des affaires de désarmement a également demandé l'avis d'entités compétentes du système des Nations Unies dans des lettres datées du 2 octobre 2023. Au 22 janvier 2024, les entités suivantes avaient présenté des observations écrites : Union internationale des télécommunications, Direction exécutive du Comité contre le terrorisme, Programme des Nations Unies pour le développement, Institut des Nations Unies pour la recherche sur le désarmement, Institut interrégional de recherche des Nations Unies sur la criminalité et la justice, Bureau de lutte contre le terrorisme, Bureau de l'informatique et des communications, Bureau des affaires juridiques et Office des Nations Unies contre la drogue et le crime.

4. Un appel à contribution a également été lancé par courrier électronique aux entités non gouvernementales concernées, le 2 octobre 2023. Au 22 janvier 2024, les entités suivantes avaient présenté des observations écrites : Association pour le progrès des communications, Centre for Communication Governance at the National Law University of Delhi, DiploFoundation, Forum mondial sur la cyber expertise, Chambre de commerce internationale, Centre of Excellence for National Security of the S. Rajaratnam School of International Studies, SafePC Solutions, Third Eye Legal, Write Pilot. L'Union européenne a également présenté sa réponse. Des observations écrites conjointes ont également été reçues des pays suivants : Argentine, Brésil, Chili, Colombie, Costa Rica, El Salvador, Équateur, Guatemala, Paraguay, République dominicaine et Uruguay. Une communication conjointe a été reçue des entités suivantes : National Cyber and Information Security Agency of Czechia, Comité international de la Croix-Rouge (CICR), Centre d'excellence de l'OTAN pour la coopération en matière de cyberdéfense, Université d'Exeter, United States Naval War College et Université de Wuhan.

5. Toutes les observations écrites reçues, y compris après le délai formel prolongé, sont disponibles sur le site Web du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025)[1]. Les États sont encouragés à consulter l'intégralité des communications écrites émanant des États Membres, des entités du système des Nations Unies et des entités non gouvernementales concernées, le présent rapport ne constituant pas un inventaire exhaustif de toutes les activités qui y sont décrites.

6. Le présent rapport s'appuie principalement sur les contributions reçues des États Membres, des entités du système des Nations Unies et des parties prenantes non gouvernementales énumérées ci-dessus, sans préjudice de leurs positions individuelles. Des informations supplémentaires provenant de sources ouvertes sont présentées afin de donner un aperçu équilibré et illustratif des programmes et initiatives de renforcement des capacités existants au sein et en dehors de l'Organisation, ainsi qu'aux niveaux mondial et régional.

7. Dans les exemples de programmes et d'initiatives de renforcement des capacités présentés, l'accent est d'abord mis sur les efforts déployés aux niveaux régional et sous-régional, les informations étant ensuite classées par thème. Ces descriptions ne constituent pas un inventaire exhaustif de toutes les initiatives et de tous les programmes de renforcement des capacités, mais visent plutôt à donner une vue d'ensemble des activités à titre d'illustration. Il n'a pas été établi d'ordre de priorité ou de classement des activités.

[1] Disponible à l'adresse suivante : https://meetings.unoda.org/meeting/57871/documents.

8. Le présent rapport se termine par des observations et des conclusions du Secrétariat destinées à aider les États à mettre en œuvre des initiatives de renforcement des capacités plus efficaces, durables et efficientes aux niveaux mondial, régional et sous-régional.

II. Aperçu des discussions et conclusions des États sur le renforcement des capacités au niveau multilatéral

9. Compte tenu de l'évolution des menaces liées à leur utilisation du numérique dans le contexte de la sécurité internationale, les États continuent de faire valoir l'urgence du renforcement de la capacité de tous les États de respecter et de mettre en œuvre le cadre cumulatif et évolutif élaboré dans ce contexte aux fins du comportement responsable des États, comme affirmé dans le deuxième rapport annuel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) (A/78/265).

10. Les États ont souligné la nécessité de promouvoir une meilleure compréhension des besoins des États en développement dans le but de réduire la fracture numérique en adaptant les efforts de renforcement des capacités. Les États ont fait valoir qu'il fallait d'urgent renforcer les capacités et les bonnes pratiques dans divers domaines diplomatiques, juridiques, politiques, législatifs et réglementaires, en plus des compétences techniques, de la mise en place d'institutions et des mécanismes de coopération. Les États ont selon le cas souligné l'importance de la coopération Sud-Sud, de la coopération triangulaire et de la coopération sous-régionale et régionale, en complément de la coopération Nord-Sud. Les États ont également rappelé l'utilité de l'approche de la formation des formateurs associée à une formation spécialisée, à des programmes d'études adaptés et à une certification professionnelle, qui permettront de transmettre les connaissances et les compétences nécessaires aux homologues concernés.

11. 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 de faire des propositions concrètes concernant les mesures à prendre pour renforcer les capacités, notamment en vue de mettre en place un portail mondial de coopération en matière de cybersécurité, notamment une proposition visant à encourager la poursuite des échanges techniques sur les menaces liées à l'informatique et aux communications afin de renforcer les capacités des États à recenser et à détecter les activités malveillantes liées aux TIC et à y répondre en connaissance de cause, et une autre proposition concernant la tenue de discussions sur la promotion d'une collaboration et de partenariats véritables avec des parties prenantes non gouvernementales dans le domaine du renforcement des capacités, y compris à des fins de formation et de recherche.

12. Le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) est lui-même reconnu comme une plateforme permettant de poursuivre l'échange de vues et d'idées sur les mesures de renforcement des capacités en matière de sécurité numérique, y compris sur la meilleure façon de tirer parti des initiatives existantes afin d'aider les États à se doter de la force institutionnelle nécessaire pour mettre en œuvre le cadre de comportement responsable dans ce domaine.

13. Les États ont continué à promouvoir l'intégration des principes guidant le renforcement des capacités liées à l'utilisation des technologies numériques par les États dans le contexte de la sécurité internationale, qui sont énoncés à l'annexe C du document A/78/265 et ont été élaborés pour la première fois dans le rapport final du

Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale[2]. En approuvant ces principes, les États ont conclu que les activités de renforcement des capacités doivent reposer sur des données factuelles, être politiquement neutres, transparentes, responsables et ne faire l'objet d'aucune condition. Ils ont en outre convenu que le renforcement des capacités devrait être entrepris dans le plein respect du principe de la souveraineté des États, être axé sur la demande, correspondre aux besoins et priorités recensés au niveau national et être respectueux des droits humains et des libertés fondamentales. Dans son deuxième rapport d'activité (A/78/265), le groupe de travail à composition non limitée a recommandé que les États élaborent et partagent, à titre volontaire, des listes de contrôle et d'autres outils permettant d'intégrer les principes convenus en matière de renforcement des capacités.

14. Dans le cadre des travaux du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), les États ont continué à sensibiliser le public à la dimension de genre de la sécurité d'utilisation du numérique et promouvoir la prise en compte de cette dimension aussi bien dans l'élaboration des politiques que dans la sélection et l'exécution des projets relatifs au renforcement des capacités. Ils ont encouragé les activités de renforcement des capacités tenant compte des questions de genre, notamment par l'intégration des questions de genre dans les politiques nationales aux TIC et les initiatives relatives au renforcement des capacités, ainsi que par l'élaboration de listes de contrôle ou de questionnaires permettant de recenser les besoins et les lacunes dans ce domaine.

15. Les États ont fait valoir que l'ONU pouvait jouer un rôle important à cet égard, notamment en faisant le point sur les besoins des États en matière de renforcement des capacités, en recensant les lacunes dans ce domaine au moyen d'outils et d'enquêtes et en facilitant l'accès des États aux programmes de renforcement des capacités, y compris grâce au présent « état des lieux ».

III. Coopération régionale, sous-régionale et interrégionale

16. Les États ont constamment réaffirmé que les organisations régionales et sous-régionales jouent un rôle important dans l'appui aux efforts visant à mettre en œuvre le cadre de comportement responsable en matière d'utilisation du numérique, notamment en soutenant les initiatives de renforcement des capacités dans ce domaine. Les États ont réfléchi de diverses manières aux mesures qui pourraient être prises aux niveaux régional, sous-régional et transrégional, y compris des ateliers, des cours de formation et des échanges sur les meilleures pratiques et les enseignements tirés. Ils ont également été encouragés à soutenir les programmes de renforcement des capacités, y compris en collaboration, selon qu'il convient, avec les organisations régionales et sous-régionales[3].

17. En ce qui concerne la coopération interrégionale, le Forum mondial sur la cyberexpertise est une communauté multipartite qui compte plus de 200 membres et partenaires, dont des États de toutes les régions, des organisations internationales et régionales et des acteurs du secteur privé, de la société civile et du monde universitaire. Le portail Cybil, initiative phare du Forum mondial sur la cyberexpertise, est un registre en ligne des projets internationaux de renforcement des capacités cybernétiques et héberge une bibliothèque de ressources pour les parties prenantes[4].

---

[2] A/75/816, annexe I, par. 56.

[3] A/78/265, annexe, par. 51.

[4] Voir https://cybilportal.org/about-cybil/.

18. En novembre 2023, le Forum mondial sur la cyberexpertise a accueilli la première conférence mondiale sur le renforcement des capacités cybernétiques, en coopération avec le Ghana, le Forum économique mondial, la Banque mondiale et l'Institut CyberPeace. Des sessions thématiques et des sessions d'analyse approfondie au niveau régional ont été organisées dans le cadre de la conférence. Le document final issu de la Conférence, l'Appel d'Accra pour un développement cyberrésilient, énonce une série de mesures d'orientations non contraignantes et facultatives qui visent à : a) renforcer le rôle de la cyberrésilience en tant que facteur clé du développement durable ; b) souligner l'importance d'un renforcement des cybercapacités axé sur la demande, efficace et durable ; c) promouvoir des partenariats plus solides et une meilleure coordination ; d) libérer des ressources financières et tirer parti de toutes les options de mise en œuvre[5]. Dans le cadre de cette conférence, il a été annoncé que la prochaine conférence mondiale sur le renforcement des cybercapacités se tiendrait à Genève en mai 2025, l'objectif étant de s'appuyer sur les progrès amorcés au Ghana.

19. Afin de renforcer la coopération entre les régions, l'Alliance numérique Union européenne – Amérique latine et Caraïbes organise des dialogues sur la réglementation et la cybersécurité, ainsi que d'autres activités sur les questions numériques et spatiales. L'objectif de l'Alliance consiste à favoriser la transformation numérique et l'innovation selon une approche des économies et des sociétés numériques centrée sur l'humain. Afin d'atteindre ces objectifs, les activités menées dans le cadre de l'Alliance prévoient l'établissement d'un dialogue birégional sur la politique numérique, l'extension du programme BELLA (Building the Europe Link to Latin America) (BELLA II), la mise en œuvre d'une stratégie régionale Copernicus destinée à renforcer la résilience numérique en soutenant la capacité de gestion des données spatiales et leur utilisation stratégique, et la mise sur pied d'un accélérateur numérique UE-ALC pour encourager l'esprit d'entreprise et l'innovation.

20. Un projet en cours intitulé « Renforcer la coopération en matière de sécurité entre l'Union européenne et l'Asie » (ESIWA), soutenu par l'Union européenne et financé par la France et l'Allemagne, vise à promouvoir une convergence accrue entre les politiques et les pratiques de l'Union européenne et des pays partenaires, à renforcer la sensibilisation et à favoriser les dialogues en matière de sécurité opérationnelle[6]. Les activités menées dans le cadre de ce projet s'articulent autour de quatre volets thématiques : lutte contre le terrorisme et prévention de l'extrémisme violent ; cybersécurité ; sécurité maritime ; gestion de crise. Les États participants sont actuellement l'Inde, l'Indonésie, le Japon, la République de Corée, Singapour et le Viet Nam.

21. Dans la région de l'Europe centrale et orientale, le Centre de développement de capacités cyber dans les Balkans occidentaux a été lancé par la France, le Monténégro et la Slovénie en mai 2023[7]. Le Centre vise à aider six pays et régions participants à renforcer leurs capacités de réponse opérationnelle et institutionnelle. Les activités incluent des cours de formation, l'élaboration de cyberprogrammes et l'échange d'informations et de bonnes pratiques pour aider les praticiens des États des Balkans occidentaux à prévenir les cybermenaces, à s'y préparer et à y riposter. En 2023, le Centre a organisé des cours de formation sur l'hygiène cybernétique à l'intention des administrations publiques, un programme de mentorat pour les femmes dans le domaine de la cyberpolitique et des négociations internationales, des cours sur la cybercriminalité pour les autorités judiciaires et les forces de police, et un cours à

[5] Disponible à l'adresse : https://gc3b.org/news/read-the-full-accra-call-for-cyber-resilient-development/.

[6] Voir https://www.eeas.europa.eu/sites/default/files/factsheet_eu_asia_security_july_2019.pdf.

[7] Voir https://cybilportal.org/projects/western-balkans-cyber-capacity-centre-wb3c/.

l'intention des responsables de la sécurité de l'information dans les infrastructures critiques. Au moment de l'établissement du présent rapport, 12 autres cours de formation étaient prévus pour 2024. De même, un projet de l'Union européenne codirigé par la Tchéquie et l'Estonie vise à soutenir le renforcement des capacités en matière de cybersécurité dans les Balkans occidentaux en promouvant : a) la gouvernance et la sensibilisation à la cybersécurité ; b) le renforcement des cadres juridiques, des normes applicables au cyberespaces et du respect du droit international ; c) la gestion des risques et des crises ; et d) les capacités opérationnelles, notamment en étayant l'équipe d'intervention en cas d'atteinte à la sécurité informatique. Un autre projet de l'Union européenne, portant sur l'alerte précoce en matière de cybersécurité pour l'Albanie, le Monténégro et la Macédoine du Nord (« Cybersecurity rapid response for Albania, Montenegro and North Macedonia ») a été mis en œuvre pour renforcer la résilience aux cyberincidents.

22. Le Département des menaces transnationales de l'Organisation pour la sécurité et la coopération en Europe (OSCE) mène des activités conçues pour renforcer les capacités des États participants de lutter contre les menaces liées à la sécurité des technologies de l'information et de la communication. L'éventail des activités comprend des exercices visant à promouvoir des ripostes nationales adéquates face aux incidents impliquant des infrastructures critiques, des ateliers sur la lutte contre l'utilisation d'Internet à des fins terroristes et des formations aux enquêtes et aux poursuites dans les affaires de cybercriminalité[8]. En 2023, le Département a organisé à Vienne un cours de formation sur la cyberdiplomatie internationale, axé sur le renforcement des capacités nationales de participer aux délibérations internationales sur la cyberpolitique. En tant que responsable de la mise en œuvre des échelles nationales de gravité des cyberincidents et des mesures connexes visant à protéger les infrastructures critiques, l'OSCE préconise l'élaboration de procédures de communication et de gestion des crises et de méthodes de classification des incidents dans les pays d'Europe, d'Asie centrale et d'autres régions. En outre, l'OSCE sert de forum multilatéral à plusieurs discussions sur la coopération dans le cyberespace et le renforcement des capacités.

23. La Fédération de Russie organise avec le Forum régional de l'Association des nations de l'Asie du Sud-Est (ASEAN) des séminaires annuels et des ateliers en ligne sur la terminologie dans le domaine de la sécurité et de l'utilisation des technologies de l'information et de la communication, la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles, le développement durable et sûr d'Internet et la criminalistique numérique. Elle a également organisé des formations sur les enquêtes relatives aux délits de détournement de fonds liés aux technologies de l'information et de la communication lors de la Conférence pour l'interaction et les mesures de confiance en Asie.

24. L'Union internationale des télécommunications (UIT), en coopération avec le Partenariat international multilatéral contre les cybermenaces, a créé le Centre régional de cybersécurité Oman-UIT, avec le soutien d'Oman[9]. Le Centre, installé dans les locaux de l'équipe d'intervention informatique d'urgence d'Oman, a pour objectif d'améliorer les capacités, l'état de préparation, les compétences et les connaissances dans les domaines de la cybersécurité, de la protection des infrastructures critiques et du renforcement des capacités dans la région arabe.

25. Le Comité interaméricain contre le terrorisme de l'Organisation des États américains (OEA), par l'intermédiaire de son programme de cybersécurité, aide les États Membres à renforcer leurs capacités techniques, politiques et diplomatiques afin

[8] Voir https://www.osce.org/secretariat/cyber-ict-security.

[9] Voir https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/oman-itu-arab-regional-cybersecurity-centre.spx.

de prévenir et d'identifier les cyberincidents, d'y riposter et de s'en relever, et de promouvoir un comportement responsable de la part des États dans le cyberespace[10]. Entre autres activités, le programme contribue à l'élaboration de stratégies nationales de cybersécurité et à la mise en place d'équipes nationales d'intervention en cas d'atteinte à la sécurité informatique. Il prévoit également la fourniture d'une assistance et d'une formation, d'outils et de guides aux décideurs politiques, à l'industrie et à la société civile et gère le réseau hémisphérique d'équipes d'intervention en cas d'atteinte à la sécurité informatique dans les Amériques, qui partage des informations et des données de renseignement sur les menaces à 29 équipes issues de 20 États membres de l'OEA. Le programme promeut également une meilleure prise en compte des questions de genre dans l'élaboration des politiques de cybersécurité et la représentation dans les processus multilatéraux.

26. Le Forum ibéro-américain de cyberdéfense a été organisé en octobre 2023 au Brésil[11]. Quelque 13 États y ont participé dans le but d'approfondir l'intégration et la coopération régionales afin de prévenir et d'identifier les cybermenaces, et d'y faire face. Les activités comprenaient des exercices de simulation, notamment l'exercice Cyber Guardian 5.0 et la conception d'une plateforme d'échange d'informations sur les logiciels malveillants.

IV. Aperçu non exhaustif et illustratif des initiatives de renforcement des capacités, par domaine d'action thématique

Droit international

27. Les États ont reconnu le besoin particulier d'initiatives de renforcement des capacités dans le domaine du droit international dans le contexte de la sécurité des technologies de l'information et des communications. Ils ont souligné l'urgence de la poursuite des efforts de renforcement des capacités, notamment dans le but de veiller à ce que tous les États soient en mesure de participer sur un pied d'égalité à l'élaboration de protocoles d'accord sur la manière dont le droit international s'applique à l'utilisation des technologies de l'information et de la communication. Des ateliers, des cours de formation et des échanges sur les meilleures pratiques aux niveaux international, interrégional, régional et sous-régional ont été organisés à cette fin. Les États ont également fait valoir l'intérêt de renforcer les capacités en vue de l'élaboration de documents de synthèse nationaux sur l'applicabilité du droit international à l'utilisation par les États des technologies de l'information et de la communication.

28. Les ressources en ligne disponibles au niveau mondial dans le domaine du renforcement des capacités en matière de droit international incluent notamment le Cyber Law Toolkit, élaboré par un consortium composé des entités suivantes : Agence nationale tchèque pour la cybersécurité et la sécurité de l'information, CICR, Centre d'excellence de l'OTAN pour la coopération en matière de cyberdéfense, Université d'Exeter, United States Naval War College et Université de Wuhan[12]. Cette panoplie de mesures, mise gratuitement à la disposition des gouvernements et des juristes, contient actuellement : a) 28 scénarios envisageant l'applicabilité du droit international aux cyberopérations ; b) des informations sur les positions nationales concernant l'application du droit international aux utilisations de l'informatique et des communications, y compris en ce qui concerne la souveraineté, la non-

[10] Voir https://www.oas.org/ext/en/security/prog-cyber.
[11] Voir https://dialogo-americas.com/articles/brazil-leads-ibero-american-cyber-defense-forum/.
[12] Voir https://cyberlaw.ccdcoe.org/wiki/Main_Page.

intervention ou ce qui constitue une attaque au sens du droit humanitaire international ; c) plus de 50 pages consacrées aux cyberincidents présentant des informations sur des attaques récentes ou des conflits armés en cours.

29. Le processus d'Oxford relatif à l'application des protections en droit international dans le cyberespace a été lancé en 2020 par l'Oxford Institute for Ethics, Law and Armed Conflict, en partenariat avec Microsoft [13]. Au moment de l'établissement du présent rapport, le processus d'Oxford avait publié cinq « déclarations d'Oxford sur les protections en droit international », qui sont le fruit de la collaboration entre des juristes internationaux du monde entier visant à définir et clarifier les règles du droit international applicables aux cyberopérations dans toute une série de contextes, notamment en ce qui concerne la protection du secteur des soins de santé et de la recherche sur les vaccins, la protection contre l'ingérence électorale et la réglementation relative aux opérations et activités d'information et aux opérations effectuées au moyen de logiciels rançonneurs.

30. En ce qui concerne l'applicabilité du droit international humanitaire au cyberespace, le CICR propose des ressources aux décideurs politiques, notamment des documents de recherche, des ateliers, des symposiums et la création d'une délégation du CICR pour le cyberespace, basée au Luxembourg et soutenue par ce pays. Parmi les exemples d'activités récentes, on peut citer le lancement d'un programme d'action humanitaire en coopération avec le Centre for Research in the Arts, Social Sciences and Humanities de l'Université de Cambridge, l'accueil d'une réunion internationale d'experts sur le droit international humanitaire et la participation croissante des civils aux activités cybernétiques et autres activités numériques lors de conflits armés organisées avec l'Académie de droit international humanitaire et de droits humains à Genève, les 28 et 29 septembre 2023 à Genève, et une table ronde sur la cyberguerre en partenariat avec la Research Society of International Law, tenue le 17 mai 2023 à Islamabad.

31. L'Australie, le Royaume des Pays-Bas et Singapour, en association avec Cyber Law International, ont coordonné l'organisation d'un cours de formation au droit international des cyberopérations à l'intention des fonctionnaires des États membres de l'ASEAN et de l'OSCE.

32. L'Agence japonaise de coopération internationale, grâce à une formation sur le renforcement des capacités en matière de droit international et l'élaboration de politiques permettant d'améliorer les mesures propres à garantir la cybersécurité, dispense aux fonctionnaires des organismes gouvernementaux et des équipes nationales d'intervention informatique d'urgence des pays en développement les connaissances et les compétences en matière de droit international et de politiques dont ils ont besoin pour élaborer et mettre en œuvre efficacement des mesures de cybersécurité.

33. Les États ont également engagé diverses consultations pour permettre un dialogue sur l'applicabilité du droit international. Par exemple, l'OEA, en coopération avec le Comité juridique interaméricain et le CICR, a organisé des consultations sur le droit international applicable au cyberespace[14]. En outre, en collaboration avec l'Institute for Law, Innovation and Technology de Temple University (Pennsylvanie) et Microsoft, le Mexique a organisé trois ateliers virtuels sur l'application du droit international au cyberespace, la promotion de règles et de normes pour un comportement pacifique et la réduction des fractures numériques. Ce projet a abouti à la publication d'un recueil multipartite de bonnes pratiques et de recommandations sur l'application du droit international au cyberespace, qui a été lancé lors de la

[13] Voir https://www.elac.ox.ac.uk/the-oxford-process/.

[14] Voir https://www.oas.org/en/sla/dil/International_Law_Applicable_to_Cyberspace_2022.asp.

sixième session de fond du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, en décembre 2023.

34. L'OSCE a organisé des cours avancés sur le droit international des cyberopérations, notamment un cours organisé du 13 au 17 février 2023 à Skopje, en coopération avec le Royaume des Pays-Bas et avec le soutien de l'Italie, de la Slovaquie, de la Suisse, de la République de Corée et du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, ainsi que de Cyber Law International.

Politiques, y compris l'élaboration de stratégies nationales

35. Dans l'annexe B de son deuxième rapport annuel sur l'état d'avancement des travaux figurant dans le document A/78/265, le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) a adopté une première liste de mesures de confiance volontaires à l'échelle mondiale. L'une de ces mesures encourage les États à continuer, sur une base volontaire, à partager des documents de réflexion, des stratégies nationales, des politiques et des programmes. En outre, les États ont reconnu l'importance de posséder les capacités requises pour mettre en place les politiques, la législation et les stratégies nécessaires à un environnement numérique sécurisé. Dans ce contexte, diverses mesures ont été prises pour renforcer les capacités et aider les États à formuler des politiques nationales, à élaborer des stratégies et à mettre en place les institutions et les structures nécessaires ayant les compétences voulues dans le domaine de l'informatique et des communications dans le contexte de la sécurité internationale.

36. Au niveau mondial, l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) organise une conférence annuelle sur la stabilité dans le cyberespace, prévoyant des discussions sur la promotion d'un cyberespace sûr et stable, sur les normes et le droit international et sur la promotion d'un dialogue multilatéral consacré aux questions de cybersécurité. Lors des éditions précédentes de cette conférence, des universitaires ont présenté des exposés thématiques pour contribuer à l'élaboration des points de vue nationaux des États, notamment sur les questions juridiques liées au règlement pacifique des différends en rapport avec l'utilisation de l'informatique et des communications par les États, ainsi que sur les questions politiques et techniques relatives à la protection des infrastructures et des services essentiels dans tous les secteurs. Les conférences précédentes se sont également concentrées sur les processus intergouvernementaux connexes sous les auspices de l'ONU. La prochaine conférence sur la stabilité dans le cyberespace aura lieu les 29 février et 1er mars 2024 à New York.

37. Les États ont également reconnu la valeur du Portail des politiques de cybersécurité de l'UNIDIR, qui permet aux États de prendre volontairement des mesures de transparence en partageant des informations, des politiques, des législations et d'autres bonnes pratiques pertinentes[15]. En décembre 2023, 1 528 documents avaient été téléchargés dans la base de données de ce portail, dont certains sont disponibles dans 55 langues, et des informations publiées au sujet de 897 projets de renforcement des capacités. Le portail a reçu environ 23 000 visites en 2023.

38. En décembre 2023, le Portail des politiques de cybersécurité a intégré près de 900 projets de renforcement des capacités provenant du portail Cybil du Forum mondial sur la cyberexpertise. L'échange de données comprend des détails sur les projets tels que le titre, les bénéficiaires, les bailleurs de fonds et les dates de début et de fin, et se fait dans les six langues officielles de l'Organisation. Cette initiative renforce la sécurité et l'utilisation des technologies de l'information et de la communication en faisant mieux connaître les ressources existantes, en facilitant la

[15] Voir https://cyberpolicyportal.org/fr.

collaboration entre les parties prenantes et en encourageant une plus grande transparence dans les mesures de renforcement des cybercapacités.

39. L'UIT, en partenariat avec la Banque mondiale, la Conférence des Nations Unies sur le commerce et le développement (CNUCED) et l'Organisation des télécommunications du Commonwealth, apporte un soutien politique à la création d'un cadre national efficace en matière de cybersécurité. À cette fin, la deuxième édition du *Guide to Developing a National Cybersecurity Strategy*, publiée par l'UIT en 2021, donne aux décideurs une vue d'ensemble du processus d'élaboration de la stratégie, en tenant compte de la situation spécifique de leur pays, ainsi que des valeurs culturelles et sociétales[16]. En outre, l'UIT propose un cours de formation en ligne à l'intention des futurs décideurs nationaux et spécialistes de la cybersécurité des secteurs public et privé, constitué de quatre modules d'apprentissage et d'un exercice de simulation en ligne conçus à partir du guide[17]. Un référentiel actualisé des stratégies nationales de cybersécurité présentant des politiques nationales, des plans d'action et d'autres éléments pertinents liés à la cybersécurité est également disponible en ligne[18].

40. Le programme de bourses d'études en cybernétique établi par l'ONU et Singapour se tient deux fois par an pour une session de six jours à l'intention de fonctionnaires sélectionnés, afin de renforcer les capacités et les réseaux en matière de politique, de stratégie et d'opérations nationales dans les domaines de la cybersécurité et de la sécurité numérique. Après les trois premières éditions du programme, deux autres sessions sont prévues pour 2024. Le programme dispose d'un réseau d'anciens boursiers de plus de 70 personnes, représentant 62 États Membres.

41. Le Royaume des Pays-Bas a financé les séances du Global Cyber Policy Dialogue avec Observer Research Foundation America. Deux ans durant, le projet a contribué à l'élaboration de stratégies nationales de cybersécurité et accueilli des dialogues régionaux sur la cyberpolitique en Asie du Sud-Est, dans les Balkans occidentaux, au Moyen-Orient et en Afrique du Nord, en Afrique australe, en Amérique latine et dans les Caraïbes. Le projet visait également à promouvoir la transformation numérique sécurisée et les partenariats public-privé, à identifier les besoins et les lacunes en matière de renforcement des capacités et à encourager l'élaboration continue de normes de comportement des États dans le cyberespace.

42. Dans le cadre du projet de pôle de développement numérique (Digital for Development Hub), l'Union européenne, l'Allemagne, Expertise France, la Fondation internationale et ibéro-américaine pour l'administration publique et les politiques gouvernementales et l'Initiative pour la Corne de l'Afrique ont collaboré à la mise en place d'une initiative en faveur du cybergouvernement et de la cybersécurité dans la région de la Corne de l'Afrique[19]. Le projet vise à aider les États participants (Djibouti, Kenya et Somalie) à renforcer la prestation de services du secteur public grâce à des canaux numériques sécurisés. Il prévoit des dialogues et des échanges d'informations par l'intermédiaire d'un comité technique régional, ainsi que l'examen des feuilles de route et des projets de numérisation en cours dans chaque État.

43. Sur le plan bilatéral, la France et le Sénégal se sont associés dans le cadre de l'école nationale de cybersécurité à vocation régionale, basée à Dakar, qui, entre autres activités, dispense des formations, renforce la coopération et sensibilise les

[16] Voir https://ncsguide.org/the-guide/.
[17] Voir https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.
[18] Voir https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.
[19] Voir https://www.fiiapp.org/en/proyectos_fiiapp/d4d-initiative-for-digital-governance-and-cybersecurity-idgc-for-the-horn-of-africa-initiative/.

États africains à la cybersécurité[20]. Autre exemple parmi les nombreux programmes bilatéraux actuels, le Portugal soutient des programmes de coopération stratégique menés dans le cadre de partenariats avec l'Angola, Cabo Verde, la Guinée-Bissau, le Mozambique, Sao Tomé-et-Principe et le Timor-Leste, qui renforcent les structures juridiques et administratives afin de prévenir et d'identifier les actes de cybercriminalité et de cyberterrorisme et les cyberincidents, et d'y riposter.

44. En Asie, le Global Cybersecurity Centre for Development, basé en République de Corée, fournit une assistance aux États qui en font la demande pour développer la cyberexpertise et la cyberrésilience dans le secteur public. Il propose des séminaires sur l'élaboration de stratégies et de cadres nationaux de cybersécurité, la mise en place et le fonctionnement d'équipes nationales d'intervention informatique d'urgence, la détection, la manière d'analyser les cyberincidents et d'y répondre et le partage d'informations sur les tendances et les menaces cybernétiques [21]. Des séminaires sur l'élaboration de stratégies de cybersécurité, le traitement des incidents, la cybersécurité et la résilience, entre autres thèmes, ont été organisés récemment au Costa Rica, en République démocratique populaire lao et en Serbie.

45. Dans le cadre de son programme de coopération en matière de technologies cybernétiques et critiques (Cyber and Critical Tech Cooperation Programme), le Ministère australien des affaires étrangères et du commerce prête son concours à sa commissaire à la sécurité en ligne afin de développer des ressources mondiales en matière de sécurité en ligne et de collaborer avec les pouvoirs publics en Asie et dans le Pacifique pour élaborer des approches nationales permettant de protéger les citoyens en ligne[22]. En partenariat avec des entreprises, des universités, la société civile, des organismes du gouvernement australien et d'autres donateurs animés du même esprit, le programme aide plus de 25 pays d'Asie du Sud-Est et du Pacifique à faire progresser et à protéger leurs intérêts collectifs dans le cyberespace.

46. Aux Amériques, dans le cadre du Sommet des dirigeants nord-américains, le Canada, le Mexique et les États-Unis d'Amérique ont participé à une table ronde sur la cybersécurité afin de renforcer la coopération entre les États participants lors de l'élaboration et de la mise en œuvre de politiques en matière de cybersécurité, tenue en janvier 2023. Du 8 au 14 octobre 2023, la Colombie et la Tchéquie ont organisé conjointement des discussions sur la convergence entre cybersécurité et intelligence artificielle, en mettant l'accent sur la législation, les politiques et les stratégies nationales.

47. L'initiative de cyberdiplomatie de l'Union européenne (Cyber Direct) contribue à un large éventail d'activités d'appui aux politiques, de recherche, de sensibilisation et de renforcement des capacités dans le domaine de la cyberdiplomatie, notamment grâce à sa boîte à outils cyberdiplomatique et à l'organisation d'un dialogue européen annuel sur la cyberdiplomatie[23]. Entre autres nombreux programmes et initiatives, Cyber Direct organise un programme de bourses pour les cyberexperts et les spécialistes du numérique de niveau intermédiaire et moins expérimentés des pays partenaires, à savoir des pays non-membres de l'Union européenne appartenant au Groupe des États d'Europe orientale, au Groupe Afrique, au Groupe des États d'Amérique latine et des Caraïbes ou au Groupe des États d'Asie et du Pacifique[24]. Toujours dans la région, une coalition rassemblant l'Allemagne, l'Estonie, la Finlande et le Luxembourg, dirigée par l'Autorité chargée du système d'information de

[20] Voir https://www.diplomatie.gouv.fr/en/country-files/senegal/news/article/regionally-oriented-national-school-for-cyber-security-opens-in-dakar-senegal.

[21] Voir https://www.kisa.or.kr/EN/201.

[22] Voir https://www.internationalcybertech.gov.au/cyber-tech-cooperation-program.

[23] Voir https://eucyberdirect.eu/.

[24] Voir https://eucyberdirect.eu/news/eu-cd-fellowship.

l'Estonie, gère et met en œuvre l'initiative CyberNet de l'Union européenne (2019-2025)[25], qui a créé une communauté de plus de 300 cyberexperts dans plus de 40 domaines de compétence afin de promouvoir le renforcement des cybercapacités.

48. Le Centre de Genève pour la gouvernance du secteur de la sécurité gère un programme de gouvernance de la cybersécurité qui aide les acteurs étatiques à élaborer des lois et des politiques en matière de cybersécurité, à étayer les cadres de responsabilité et à renforcer les capacités[26]. Un projet récent a permis de créer un réseau de recherche sur la cybersécurité dans les Balkans occidentaux qui, entre autres activités, mène des recherches sur la cybersécurité et les droits humains, les besoins des groupes vulnérables en matière de cybersécurité et les questions de genre, dans le contexte national de chaque pays. Le Geneva Centre for Security Policy propose également des cours et des ateliers de formation à la cybersécurité[27]. Également basée à Genève, DiploFoundation contribue au développement des capacités dans les domaines de la gouvernance d'Internet et de la politique numérique en proposant des cours en ligne, des ateliers et des exercices de simulation sur la cybersécurité, les données, l'intelligence artificielle et d'autres questions émergentes, ainsi qu'en promouvant et en développant des outils numériques propices à gouvernance et des politiques inclusives et efficaces[28].

49. Le projet Cyberspace4All, soutenu par le Royaume des Pays-Bas, vise à promouvoir l'inclusivité et la sensibilisation en créant un langage et des références communes sur la cybergouvernance internationale, en sensibilisant aux principaux faits nouveaux à l'ONU concernant les questions cybernétiques et en aidant à éclairer les politiques des États sur les cybernormes. Dans sa première phase, le projet a abouti à la publication d'un numéro du *Journal of Cyber Policy* et à la production de courtes vidéos sur le renforcement des cybercapacités et d'un podcast intitulé « Who rules cyberspace ? ». La deuxième phase, mise en œuvre conjointement avec Chatham House, vise à formuler des recommandations sur les normes et principes de l'ONU en matière de renforcement des capacités et de comportement responsable des États dans le cyberespace, à les faire connaître et à en promouvoir l'application.

50. Le renforcement des capacités dans le domaine de la cyberdiplomatie a également été proposé par le biais de différents canaux. Par exemple, l'université d'été de Tallinn sur la cyberdiplomatie est organisée dans le cadre du programme « Multilatéralisme et numérisation », en coopération avec le Ministère des affaires étrangères de l'Estonie, l'Académie de gouvernance en ligne et le Centre estonien pour le développement international. Son principal objectif est de former les diplomates qui se consacrent à la politique étrangère en matière de cybernétique, ainsi que d'autres fonctionnaires intéressés par les questions complexes liées à la cybernétique. Le programme de cybersécurité du Comité interaméricain contre le terrorisme de l'OEA propose également un programme de formation à la cyberdiplomatie pour aider les fonctionnaires travaillant dans ce domaine. Du côté du Secrétariat de l'Organisation des Nations Unies, le cours de cyberdiplomatie en ligne actuellement disponible sur la plateforme consacrée à l'éducation au désarmement sera mis à jour en 2024[29].

[25] Voir https://www.eucybernet.eu/.
[26] Voir https://www.dcaf.ch/cybersecurity-governance.
[27] Voir. https://www.gcsp.ch/.
[28] Voir https://www.diplomacy.edu/.
[29] Voir https://cyberdiplomacy.disarmamenteducation.org/home/.

Équipes d'intervention informatique d'urgence, formation technique et autre soutien connexe

51. Les États ont constamment rappelé la nécessité d'une approche du renforcement des capacités qui soit concrète et orientée vers l'action. Ils ont conclu que ces mesures concrètes pourraient inclure la fourniture d'un soutien aux équipes d'intervention informatique d'urgence ou aux équipes d'intervention en cas d'atteinte à la sécurité informatique et la mise en place d'une formation spécialisée et de programmes d'études adaptés, y compris des programmes de formation des formateurs et de certification professionnelle. Ils se sont également dits préoccupés par le fait qu'un manque d'information et de capacités s'agissant de détecter les attaques informatiques, de s'en défendre ou d'y répondre pouvait les rendre plus vulnérables.

52. L'importance de la formation technique du personnel dans le domaine du numérique a également été soulignée, s'agissant notamment de la sécurité de l'information, des méthodes de détection et de répression des attaques visant les réseaux informatiques dans les systèmes d'information ouverts, des tactiques, techniques et procédures de protection de l'information contre les accès non autorisés, de la collecte de données de sources ouvertes, des techniques d'enquête sur les crimes liés aux technologies de l'information et de la communication en relation avec la paix et la sécurité internationales et de la coopération internationale dans ce domaine, de la criminalistique informatique, de la lutte contre l'utilisation des technologies de l'information et de la communication et des services postaux internationaux aux fins du trafic de drogue et du vol de fonds, et de l'identification des transactions illégales effectuées au moyen d'actifs numériques, y compris les cryptomonnaies, de leur utilisation aux fins du financement du terrorisme et de l'engagement de poursuites à cet égard.

53. Au niveau mondial, l'UIT offre aux États une assistance permanente pour la mise en place d'équipes nationales d'intervention informatique d'urgence [30]. Récemment, de telles équipes ont été lancées dans les pays suivants, avec l'aide de l'UIT : Bahamas, Barbade, Burkina Faso, Chypre, Côte d'Ivoire, Gambie, Ghana, Jamaïque, Kenya, Kirghizistan, Liban, Malawi, Monténégro, Ouganda, République-Unie de Tanzanie, Trinité-et-Tobago et Zambie. Dans chaque cas, ces équipes servent d'organe central de coordination pour identifier les cybermenaces, les gérer et y riposter.

54. Le forum des équipes d'intervention en cas d'incidents liés à la sécurité informatique (Forum of Incident Response and Security Teams) maintient un réseau de plus de 700 équipes d'intervention informatique d'urgence participantes pour contribuer à la coopération et répondre de manière proactive et réactive aux incidents de cybersécurité. Entre autres activités, le Forum partage les pratiques optimales entre ses membres et encourage l'organisation de colloques techniques, de cours, de publications, de services Web, de groupes d'intérêt spéciaux et d'une conférence annuelle sur les interventions en cas d'incidents[31].

55. Le Secrétaire du Ministère de l'électronique et des technologies de l'information de l'Inde, Alkesh Kumar Sharma, dans le cadre de la présidence indienne du Groupe des 20, a lancé l'exercice de cybersécurité du Groupe des 20, qui a réuni plus de 400 participants nationaux et internationaux. L'équipe indienne d'intervention informatique d'urgence a organisé l'exercice de cybersécurité selon un format hybride. Des participants internationaux d'une douzaine de pays s'y sont joints en ligne. Des participants nationaux issus de secteurs tels que la finance, l'éducation, les

[30] Voir https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.
[31] Voir https://www.first.org/.

télécommunications, les ports et le transport maritime, l'énergie et les technologies de l'information et de la communication ont participé en personne et virtuellement.

56. Au cours de son mandat de président en exercice du Commonwealth, le Royaume-Uni a mené une série d'activités de renforcement des capacités dans le cadre du programme de cybersécurité du Commonwealth, à l'appui des objectifs de la déclaration de 2018 sur la cybersécurité du Commonwealth[32]. Ce programme a aidé les États membres du Commonwealth à réaliser des auto-évaluations des capacités nationales en matière de cybersécurité et permis d'offrir une assistance technique, des formations et des conseils sur les menaces liées à la cybersécurité et à la cybercriminalité. Dans le cadre de ce projet, plus de 140 activités ont été organisées dans 32 pays, et plus de 6 000 personnes ont bénéficié d'une formation.

57. Le centre d'excellence pour la cybersécurité ASEAN-Singapore offre un soutien aux États membres de l'ASEAN afin de promouvoir le renforcement des cybercapacités dans la région, grâce à des recherches, des formations, un appui technique lié aux équipes d'intervention informatique d'urgence, à l'échange d'informations sur les cybermenaces, les attaques et les meilleures pratiques, et à des formations et des exercices[33]. Depuis sa création, le centre d'excellence a organisé plus de 50 programmes auxquels ont participé plus de 1 600 hauts fonctionnaires des États participants. À partir de 2024, ses programmes seront accessibles aux États situés à l'extérieur de la région de l'ASEAN. Pour encourager une coordination et une coopération régulières, le groupe de travail d'experts sur la cybersécurité de la Réunion des ministres de la défense de l'ASEAN-Plus s'est réuni régulièrement depuis 2016 pour servir de cadre au renforcement de la confiance et à l'élaboration de normes entre les États membres de l'ASEAN.

58. Le programme de l'ASEAN pour la cybercapacité vise à renforcer les capacités des États membres en renforçant la résilience et les ripostes régionales aux menaces[34]. Les activités comprennent des ateliers, des séminaires, la semaine internationale du cyberespace à Singapour, un atelier conjoint États-Unis-Singapour sur la cybersécurité et la conférence ministérielle de l'ASEAN sur la cybersécurité. Le programme Singapore Cyber Leadership and Alumni a été lancé lors de la huitième semaine internationale du cyberespace de Singapour en 2023. Ouvert aux candidats de tous les États, il propose aux fonctionnaires des cours de base, des cours avancés et des cours de perfectionnement pour approfondir leur connaissance des concepts et des processus de cyberdiplomatie, du droit international, des normes relatives au cyberespace et des considérations opérationnelles et techniques de la politique internationale en matière de cybernétique. En outre, la création d'une bourse pour les cyberleaders (« Cyber Leaders' Alumni Fellowship ») est envisagée pour mettre en relation les anciens participants aux activités de renforcement des capacités organisées par le Centre d'excellence en matière de cybersécurité lors d'une série de réunions à huis clos sur les tendances et le discours international sur la cybersécurité, et pour échanger les meilleures pratiques dans des domaines tels que le perfectionnement de la main-d'œuvre et le renforcement des compétences, les cadres juridiques et les cybercomportements responsables.

59. La République de Corée accueille la Cybersecurity Alliance for Mutual Progress depuis son lancement en 2016. L'Alliance s'attache à promouvoir la coopération et le

---

[32] Voir https://assets.publishing.service.gov.uk/media/60538ad98fa8f55d38ea34c3/UK_Commonwealth_Cyber_Security_Programme_six_case_studies.pdf.

[33] Voir https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence.

[34] Voir https://www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0#:~:text=Cyber%20Capacity%20Programme-

renforcement des capacités entre les États participants [35]. Au moment de l'établissement du présent rapport, 67 organisations issues de 49 pays en étaient membres.

60. En 2023, l'Agence coréenne pour la sécurité sur Internet a lancé le projet de cyberbouclier de l'ASEAN, en coopération avec l'université nationale de Kangwon, l'université de Gangneung Wonju et l'université de technologie de Brunei. Ce projet vise à renforcer la coopération entre les États membres de l'ASEAN en matière de cybersécurité, à rendre opérationnel un programme d'études en ligne sur la cybersécurité dans la région, à la conduite de recherches sur les systèmes de certification en matière de cybersécurité et à l'organisation de *hackathons* de l'ASEAN et d'échanges d'étudiants en cybersécurité[36].

61. De 2017 à 2019, l'UIT a mené un projet destiné à aider les petits États insulaires du Pacifique à créer des cadres nationaux, sous-régionaux et régionaux de cybersécurité et à renforcer les compétences en la matière. Le programme visait à déterminer l'état de préparation à la mise en place d'équipes nationales d'intervention informatique d'urgence en Papouasie-Nouvelle-Guinée, à Samoa, à Tonga et à Vanuatu, et à concevoir et développer des plans de mise en œuvre pour ces équipes. Dans le cadre de ce projet, l'UIT a organisé des ateliers de formation pour renforcer la sensibilisation et les compétences, qui ont permis à plus de 200 participants et plus de 70 organisations de partager leurs expériences dans le domaine de la riposte aux incidents et de la protection des infrastructures d'information critiques. Un bilan a été effectué, dont les résultats ont ensuite été mesurés par rapport aux indicateurs du modèle de maturité des capacités en matière de cybersécurité pour les pays mis au point par le Global Cyber Security Capacity Centre de l'Oxford Martin School (Université d'Oxford)[37].

62. Le réseau opérationnel pour la cybersécurité du Pacifique[38], qui relève du programme australien de coopération en matière de technologies cybernétiques et critiques, est un réseau opérationnel d'experts régionaux en cybersécurité. Il tient un registre des points de contact opérationnels en matière de cybersécurité et permet à ses membres de partager des informations sur les menaces en matière de cybersécurité, offre aux experts techniques la possibilité d'échanger des outils, des techniques et des idées, et favorise la coopération et la collaboration, en particulier lorsqu'un incident de cybersécurité touche la région.

63. Diverses activités bilatérales axées sur les capacités techniques ont également été entreprises. Par exemple, le programme néo-zélandais de renforcement des capacités en matière de cybersécurité dans le Pacifique apporte un soutien bilatéral aux États insulaires du Pacifique pour l'élaboration de stratégies nationales de cybersécurité, le renforcement des capacités des équipes d'intervention informatique d'urgence, la sensibilisation, l'élaboration d'une législation sur la cybersécurité et la cybercriminalité qui soient conforme aux normes internationales, et l'ouverture d'enquêtes et de poursuites dans le respect de cette législation. Le colloque international sur la riposte à la cybercriminalité, qui s'est tenu en République de Corée du 13 au 15 septembre 2023, et la conférence sur le renforcement des capacités et de la coopération en matière de la cybercriminalité dans le Pacifique, qui s'est tenue

---

,Le%20ASEAN%20Cyber%20Capacity%20Programme%20(ACCP)%20vise%20à%20construire%20un%20cyber,20%20sécurisé%20et%20resilient%20ASEAN%20cyberspace.

[35] Voir https://www.cybersec-alliance.org/camp/index.do.

[36] Voir https://wwwk.kangwon.ac.kr/english/contents.do?key=2356&.

[37] Voir https://gcscc.ox.ac.uk/the-cmm.

[38] Voir https://pacson.org/.

à Fidji du 2 au 4 octobre 2023, comptent parmi les manifestations récemment organisées dans la région.

64. Dans le cadre du programme australien de coopération en matière de technologies cybernétiques et critiques, l'Australie aide ses partenaires dans le Pacifique et en Asie du Sud-Est à renforcer leur capacité de résistance aux cybermenaces sur le plan technique et sur le plan de la gouvernance[39]. Établi en 2016, le programme de coopération a été élargi en 2021 pour inclure la coopération en matière de technologies critiques. En novembre 2023, le programme avait soutenu 126 projets dans 21 pays de la région. Les projets comprennent des activités destinées à renforcer les capacités en matière de cybersécurité, à mettre la technologie au service de la croissance économique et du développement, à préconiser la protection des droits humains et de la démocratie en ligne, à prévenir la cybercriminalité et à en poursuivre les auteurs, et à appuyer la mise en œuvre du cadre normatif élaboré pour promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationales approuvé par l'ONU. Le projet Cyber Bootcamp, lancé en août 2019 dans le cadre du programme de coopération, a été conçu pour dispenser aux représentants des pouvoirs publics partout en Asie du Sud-Est des compétences spécialisées et une formation pratiques sur les difficultés et les possibilités communes.

65. Le Centre de compétence en cybernétique pour l'Amérique latine et les Caraïbes, créé en 2022, soutenu par l'Union européenne et basé en République dominicaine, propose aux États d'Amérique latine et des Caraïbes des formations et des activités de renforcement des capacités en matière de cybersécurité et de cybercriminalité. Ces activités incluent du matériel de formation et des cours, la sensibilisation des décideurs politiques à la cybersécurité nationale et à la transformation numérique et un appui connexe, ainsi que des consultations nationales et régionales sur les questions de cybersécurité. Des efforts bilatéraux ont également été déployés pour contribuer à la mise en place d'équipes nationales d'intervention informatique d'urgence, notamment un projet de l'Agence brésilienne de coopération en faveur de la création au Suriname d'un centre d'intervention en cas d'incident de cybersécurité.

66. De 2016 à 2019, le Programme mondial de renforcement des capacités en matière de cybersécurité, financé par le Fonds de partenariat Corée-Banque mondiale, a fourni une assistance technique nationale et régionale sur mesure à l'Albanie, à la Bosnie-Herzégovine, au Ghana, au Kirghizistan, au Myanmar et à la Macédoine du Nord[40]. Chaque État participant a fait l'objet d'une évaluation d'après le Modèle de maturité des capacités en matière de cybersécurité pour les pays, qui a servi de base à l'élaboration de rapports analytiques et à l'organisation de formations, d'ateliers et de l'octroi d'une assistance technique. Le projet visait à aider les États participants à renforcer l'environnement national de cybersécurité, avec la collaboration des décideurs politiques et des parties prenantes. Les études d'impact ont permis de mesurer l'efficacité des interventions.

Autres domaines de renforcement des capacités

67. Les efforts de renforcement des capacités dans d'autres domaines transversaux et thématiques se poursuivent, notamment auprès de groupes spécifiques tels que les femmes, les jeunes, les universitaires et l'industrie. La sensibilisation du public, l'accès au numérique, la culture numérique et la lutte contre la cybercriminalité comptent parmi les autres domaines d'intervention.

[39] Voir https://www.internationalcybertech.gov.au/our-work/capacity-building.
[40] Voir https://www.worldbank.org/en/news/feature/2020/06/01/kwpfgscp.

Questions de genre et participation des femmes

68. Lancé en 2020, le programme de bourse « Women in International Security and Cyberspace Fellowship » est une initiative conjointe de l'Australie, du Canada, des États-Unis, de la Nouvelle-Zélande, du Royaume des Pays-Bas et du Royaume-Uni[41]. Il promeut la participation des femmes diplomates aux sessions des processus intergouvernementaux connexes sous les auspices de l'ONU, notamment du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, et organise des formations et des ateliers sur les techniques de négociation. Pour sa deuxième édition, le programme permet à 35 femmes diplomates représentant des pays de l'ASEAN, de l'Asie et du Pacifique, de l'Amérique du Sud et du Commonwealth de participer aux réunions du groupe de travail à composition non limitée. Les boursières reçoivent également une formation de l'Institut des Nations Unies pour la formation et la recherche consacrée aux négociations multilatérales, participent à une présentation des questions relatives à la sécurité internationale dans le cyberespace et bénéficient du mentorat de collègues chevronnés travaillant sur ces questions au Siège de l'ONU, à New York.

69. L'UIT gère actuellement un programme intitulé « Her Cybertracks » qui vise à promouvoir une représentation égale, complète et véritable des femmes dans le domaine de la cybersécurité[42]. Ce programme aide les participantes à acquérir les compétences nécessaires pour participer à l'élaboration des politiques nationales et internationales en matière de cybersécurité, à accroître la sensibilisation et à réduire les obstacles à la participation des femmes dans ce domaine, ainsi qu'à élargir la participation et la représentation des femmes dans le secteur de la cybersécurité. En Asie du Sud-Est, l'UIT a réalisé un projet destiné à favoriser l'élaboration de normes et de cadres concernant les technologies essentielles qui favorisent la participation et l'intégration des femmes et le renforcement de leurs moyens d'action. Ce projet encourage l'élaboration de politiques, de normes, de cadres et d'initiatives visant à atténuer les préjugés et à renforcer la confiance et l'inclusion. Il a été déployé dans un premier temps en Indonésie, en Malaisie, aux Philippines et en Thaïlande, dans la perspective d'être étendu à d'autres États de la région.

70. L'UIT propose également un programme de mentorat pour les femmes dans le domaine du cyberespace. La première édition a été lancée en 2021 à l'occasion de la Journée internationale des femmes et organisée conjointement par l'UIT, le forum des équipes d'intervention en cas d'incidents liés à la sécurité informatique (Forum of Incident Response and Security Teams) et le Partenariat mondial pour l'égalité femmes-hommes à l'ère numérique (également appelé « Égaux »). Depuis sa création, près de 300 femmes ont été formées et encadrées dans 73 pays.

Participation des jeunes et sensibilisation

71. Afin de sensibiliser les jeunes à la sécurité du numérique, de les impliquer et de renforcer leurs capacités, l'équipe d'intervention informatique d'urgence de Türkiye a organisé un concours en ligne de 24 heures sur la cybersécurité, appelé « Cyber Star ». Plus de 20 000 participants ont concouru lors de l'édition 2019, en équipe ou individuellement. L'équipe d'intervention informatique d'urgence gère également un cyberprogramme, appelé « FETİH », qui vise à développer les compétences des stagiaires souhaitant travailler dans ce domaine.

[41] Voir https://eucyberdirect.eu/good-cyber-story/women-and-international-security-in-cyberspace-fellowship.

[42] Voir https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/HerCyberTracks/Her-CyberTracks.aspx.

72. Certains États ont fait état d'initiatives lancées au niveau national pour sensibiliser à l'importance des bonnes pratiques dans le domaine de la cybersécurité. Par exemple, au cours du mois d'octobre, la Garde nationale du Mexique promeut des activités dans le cadre d'une semaine nationale de la cybersécurité, qui vise à rassembler des représentants de tous les secteurs concernés pour partager de bonnes pratiques et des expériences concernant la protection des infrastructures critiques, la sécurité des citoyens dans le cyberespace, l'économie numérique, la vie privée et l'harmonisation des cadres législatifs nationaux.

Collaboration avec l'industrie et le secteur privé

73. Les États ont selon le cas souligné la valeur des partenariats public-privé et de la collaboration avec des partenaires industriels pour renforcer la cyberrésilience. Ils ont fait part des mesures prises pour mener des consultations avec des organisations publiques et privées clés afin d'évaluer le niveau général de cybersécurité nationale. En octobre 2023, la conférence sur la cybersécurité de Kouban a accueilli des représentants d'établissements d'enseignement supérieur, des autorités nationales et municipales, des chefs d'entreprises liées aux infrastructures de la Fédération de Russie et des membres de la communauté internationale, venus discuter des enjeux, des tâches et des tendances. Cette manifestation a également été l'occasion d'un concours axé sur la jeunesse intitulé « KubanCTF-2023[43] ».

74. Google a élaboré un document d'orientation sur la cybersécurité à l'intention des États, en s'inspirant des enseignements tirés et des pratiques optimales quant à la mise au point de solutions globales de sécurité et d'informatique basée sur le cloud pour les gouvernements et les particuliers. L'objectif de ce document est d'aider les États à élaborer des stratégies nationales de cybersécurité pour protéger les infrastructures critiques, les citoyens et la prospérité économique[44].

Ressources et études des institutions académiques

75. Le programme de La Haye sur la cybersécurité internationale produit des recherches sur les faits nouveaux dans le domaine numérique et sur les normes cybernétiques, organise une conférence universitaire annuelle et tient un répertoire sur les recherches et les discussions théoriques[45]. Les publications récentes couvrent des thèmes tels que l'engagement multipartite dans les processus d'élaboration de normes de cybersécurité et le comportement responsable dans le cyberespace.

76. Le Modèle de maturité des capacités en matière de cybersécurité pour les pays définit cinq dimensions de la maturité et les étapes nécessaires pour y parvenir. Il a été déployé plus de 130 fois dans plus de 90 États depuis 2015, facilité par le Global Cyber Security Capacity Centre en coopération avec des organisations internationales, régionales et d'autres organisations partenaires. Pour ce qui est de l'avenir, le centre a entrepris de mettre au point, dans le cadre du modèle, un indicateur supplémentaire permettant de mesurer les capacités en matière d'intelligence artificielle, afin d'aider les États à s'adapter à celle-ci et à l'utiliser de manière sûre et durable.

Développement, accès et culture numériques

77. Le Programme des Nations Unies pour le développement (PNUD) déploie diverses initiatives pour soutenir la mise en place d'infrastructures numériques, la promotion de la culture numérique ou la mise en œuvre de solutions de gouvernance

[43] Voir https://kubcsc.ru/en#events.
[44] Voir https://safety.google/intl/en_uk/.
[45] Voir https://www.thehagueprogram.nl/.

en ligne[46]. Il a introduit l'évaluation de la préparation numérique dans le but d'identifier et de prioriser les interventions numériques dans le cadre de la transformation numérique d'un pays. Cette évaluation met en évidence le contexte numérique actuel du pays concerné – depuis le cas où les fondements numériques de base peuvent être absents ou incomplets, jusqu'au cas d'un pays où le numérique est un principe central de la croissance et du développement nationaux (les stades de préparation numérique).

78. Le programme d'accès numérique du Gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord cherche à catalyser un accès numérique plus inclusif, abordable, sûr et sécurisé pour les communautés en Afrique du Sud, au Brésil, en Indonésie, au Kenya et au Nigéria[47].

79. L'initiative pour l'administration numérique et la cybersécurité dans les pays de la Corne de l'Afrique soutient les gouvernements de Djibouti, du Kenya et de la Somalie dans le renforcement de la gouvernance électronique et le développement de services électroniques centrés sur l'humain. En juillet 2023, en partenariat avec Smart Africa et par l'intermédiaire de la Smart Africa Digital Academy, le Burkina Faso a organisé des formations certifiantes en informatique en nuage et en cybersécurité.

80. L'initiative « Cyber4Good » de l'UIT vise à faciliter l'accès aux services et outils numériques dans les pays les moins avancés, avec la participation d'acteurs du secteur privé et le soutien de la République de Corée[48]. Le projet aboutira notamment à la création d'un fonds d'affectation spéciale pour la cybersécurité de l'UIT, fonctionnant selon un modèle de gouvernance et sous la direction d'un conseil consultatif. Le programme Cyber Resilience for Development de l'Union européenne aide les acteurs publics et privés dans le renforcement de la cybersécurité et de la résilience à l'échelle mondiale[49].

81. Le programme de partenariat pour le développement numérique de la Banque mondiale encourage la transformation numérique inclusive dans plus de 80 pays[50]. Le Fonds d'affectation spéciale multidonateur pour la cybersécurité, lancé en 2021 et financé par l'Allemagne, l'Estonie, le Japon et les Pays-Bas (Royaume des), étaye le programme de développement numérique par la recherche, l'appui aux programmes, l'évaluation et l'atténuation des risques dans les infrastructures critiques et les secteurs à haut risque. En coopération avec l'Union africaine, l'initiative de la Banque mondiale en faveur d'une économie numérique pour l'Afrique soutient la mise en œuvre de la Stratégie de transformation numérique pour l'Afrique (2020-2030). S'appuyant sur des piliers fondamentaux tels que l'infrastructure, les services et les compétences numériques, un environnement politique et réglementaire favorable, l'innovation et l'esprit d'entreprise, la stratégie fait de la cybersécurité, de la vie privée et de la protection des données à caractère personnel un thème transversal. Elle présente des propositions détaillées visant à renforcer les capacités en matière de développement numérique, d'accès et d'alphabétisation, y compris la promotion du renforcement des capacités humaines et institutionnelles grâce à des campagnes de sensibilisation du public, à la formation professionnelle, à la recherche et au développement et aux équipes d'intervention informatique d'urgence[51].

---

[46] Voir https://www.undp.org/digital.

[47] Voir https://www.oecd.org/cooperation-developpement-apprentissage/pratiques/ne-laisser-personne-de-cote-dans-un-monde-numerique-le-programme-du-royaume-uni-sur-l-acces-au-numerique-7c2000ff/.

[48] Voir https://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=2GLO21119.

[49] Voir https://cyber4dev.eu/.

[50] Voir https://www.digitaldevelopmentpartnership.org/.

[51] Voir https://www.worldbank.org/en/programs/all-africa-digital-transformation.

Lutte contre la cybercriminalité

82. Le Programme mondial contre la cybercriminalité de l'Office des Nations Unies contre la drogue et le crime a été créé en 2013. Son mandat est défini dans la résolution 65/230 de l'Assemblée générale et dans les résolutions 22/7 et 22/8 de la Commission pour la prévention du crime et la justice pénale. Le Programme mondial fonctionne sur la base de ces résolutions, mais il convient de noter qu'un traité est actuellement négocié par l'Assemblée générale. Il aborde les aspects interdépendants de la lutte contre la cybercriminalité : la prévention, la détection, l'enquête, les poursuites et la condamnation ou le jugement.

83. L'Organisation internationale de police criminelle (INTERPOL), par l'intermédiaire de son Centre de fusionnement sur la cybercriminalité multipartite, dirige actuellement l'élaboration et la fourniture d'une assistance technique et le renforcement des capacités propres aux services répressifs dans le domaine des technologies de l'information et de la communication et de la cybercriminalité. Le Centre aide les pays membres à identifier les cybermenaces, à élaborer des stratégies pour les désorganiser et à coordonner les ripostes.

Lutte contre l'utilisation de l'informatique et des communications à des fins terroristes

84. Le Programme mondial antiterroriste sur la cybersécurité et les nouvelles technologies aide les États membres et les organisations internationales et régionales à élaborer et à mettre en œuvre des réponses efficaces aux nouveaux défis et aux nouvelles possibilités associés aux nouvelles technologies de l'information et des communications dans la lutte contre le terrorisme. Il vise à développer les connaissances et la sensibilisation, ainsi qu'à renforcer les compétences et les capacités nécessaires pour mettre en œuvre des réponses politiques, protéger les infrastructures critiques contre les activités terroristes faisant appel à l'informatique et aux communications, et à donner davantage de moyens à la justice pénale. Plus de 4 000 fonctionnaires originaires de 150 États Membres ont ainsi été formés grâce à plus de 60 ateliers de renforcement des capacités, et 12 supports de connaissance ont été publiés dans le cadre du programme. Une aide au renforcement des capacités en matière de cybersécurité, sous la forme de cyber exercices de lutte contre le terrorisme et d'exercices de simulation, a également été apportée dans le cadre du programme.

V. Observations et conclusions du Secrétariat

85. Le renforcement des capacités en matière d'informatique et de communications dans le contexte de la sécurité internationale reste à juste titre l'une des principales priorités des États. Il sous-tend largement les efforts entrepris dans tous les domaines connexes traités par le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), à savoir la lutte contre les menaces existantes et émergentes, l'analyse de l'applicabilité du droit international à l'utilisation de ces technologies par les États et la promotion des mesures de confiance. De nombreux États ont également souligné l'importance d'aborder la question du renforcement des capacités dans tout futur dialogue institutionnel régulier sur la sécurité de l'informatique et des communications organisé sous les auspices de l'ONU. **À cet égard, le renforcement des capacités devrait rester une composante fondamentale et transversale de toutes les discussions sur la sécurité de l'informatique et des communications menées par les États au sein de l'Organisation. Pour progresser dans tous les domaines concernés, de l'élaboration des normes au droit international en passant par les mesures de**

confiance, il faudra consacrer des ressources à la mise en œuvre des mesures de renforcement des capacités correspondantes.

86. Le Secrétaire général a souligné qu'il est crucial d'investir dans la culture et l'infrastructure numériques pour réduire la fracture numérique (A/75/982). De même, les États ont continué à souligner que les avantages de la technologie numérique n'étaient pas les mêmes pour tous et ont donc insisté sur la nécessité d'accorder l'attention voulue à la fracture numérique croissante dans le contexte de l'accélération de la mise en œuvre des objectifs de développement durable, tout en respectant les besoins et les priorités nationaux des États. **Il est donc essentiel que le renforcement des capacités dans le domaine de l'informatique et des communications réponde effectivement aux besoins et aux priorités de tous les États, en particulier des pays en développement, afin de réduire la fracture numérique, y compris entre les genres. Le renforcement des capacités devrait également servir de catalyseur au développement durable**.

87. L'effet des progrès rapides de la science et de la technologie sur la paix et la sécurité internationales n'est pas encore totalement connu. Les possibilités et les risques créés par le développement rapide des technologies émergentes, notamment l'intelligence artificielle et les technologies quantiques, devraient avoir de profondes répercussions sur les besoins et les priorités des États en matière de renforcement des capacités aux niveaux technique et politique. D'une part, l'utilisation des technologies de l'information et de la communication, telles que l'amélioration de la détection et de l'analyse des menaces, l'intervention automatisée en cas d'incident, l'amélioration de la détection des logiciels malveillants et les outils de détection et de prévention des fraudes, nécessite des moyens accrus. D'autre part, les mesures de renforcement des capacités sont essentielles pour donner aux États les connaissances et les compétences permettant de relever des défis tels que les activités malveillantes liées à l'informatique et aux communications fondées sur l'intelligence artificielle, les préjugés et la discrimination inhérents aux systèmes d'intelligence artificielle, et les questions de transparence. **Les initiatives concrètes de renforcement des capacités pourraient privilégier l'acquisition de connaissances et d'expertise sur les incidences de ces technologies émergentes, sur l'élaboration de stratégies nationales relatives à la conception, au développement et à l'utilisation responsables des technologies émergentes, et sur les mécanismes de coopération internationale permettant de renforcer la cyberrésilience grâce au transfert de connaissances, de bonnes pratiques et d'enseignements tirés de l'expérience**.

88. Les possibles chevauchements d'activités restent un enjeu permanent au regard de l'efficacité et de la durabilité des mesures de renforcement des capacités. Dans ce contexte, il convient de noter que dans la décision 630 du Conseil de l'Union internationale des télécommunications, adoptée en août 2023, l'UIT a été chargée de mettre en place une ressource pour les États Membres comprenant notamment des renseignements sur les programmes de renforcement des capacités qu'elle met en œuvre, ainsi que sur d'autres programmes pertinents[52]. Il a été demandé que cette ressource soit tenue à jour afin de tenir compte des défis qui se font jour et des faits nouveaux. Les États ont régulièrement soulevé la question de l'exploitation des synergies et du parti à tirer des initiatives existantes à cet égard. **Compte tenu du caractère universel du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, les États sont encouragés à utiliser le processus intergouvernemental prévu à cet effet pour approfondir la question de savoir comment éviter les chevauchements d'activités en vue d'assurer la meilleure adéquation possible entre les besoins et les ressources**.

[52] Disponible à l'adresse suivante : https://www.itu.int/md/S23-CL-C-0124/fr.